(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 107 137 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
13.06.2001 Bulletin 2001/24

(51) Int Cl.7: **G06F 17/30**

(21) Application number: **00310981.6**

(22) Date of filing: **08.12.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **09.12.1999 US 457563**
20.01.2000 US 487417

(71) Applicant: **International Business Machines Corporation**
Armonk, NY 10504 (US)

(72) Inventors:
- **Mourad, Magda, c/o IBM United Kingdom Ltd.**
Winchester, Hampshire SO21 2JN (GB)
- **Munson, Jonathan P., c/o IBM United Kingdom Ltd.**
Winchester, Hampshire SO21 2JN (GB)
- **Pacifici, Giovanni, c/o IBM United Kingdom Ltd.**
Winchester, Hampshire SO21 2JN (GB)
- **Tantawy, Ahmed, c/o IBM United Kingdom Ltd.**
Winchester, Hampshire SO21 2JN (GB)
- **Youssef, Alaa S., c/o IBM United Kingdom Ltd.**
Winchester, Hampshire SO21 2JN (GB)

(74) Representative: **Ling, Christopher John**
IBM United Kingdom Limited,
Intellectual Property Department,
Hursley Park
Winchester, Hampshire SO21 2JN (GB)

(54) Digital content distribution using web broadcasting services

(57) A method of securely receiving data on a user's system from a web broadcast infrastructure with a plurality of channels. The method comprising the steps of: receiving promotional metadata from a first web broadcast channel, the promotional metadata related to data available for reception; assembling at least part of the promotional metadata into a promotional offering for review by a user; selecting by a user, data to be received related to the promotional metadata; receiving data from a second web broadcast channel, the data selected from the promotional metadata, and wherein the data has been previously encrypted using a first encrypting key; and receiving the first decrypting key via a computer readable medium, the first decrypting key for decrypting at least some of the data received via the second web broadcast channel. In another embodiment, a method and system to transmit data securely from a web broadcast centre is disclosed.

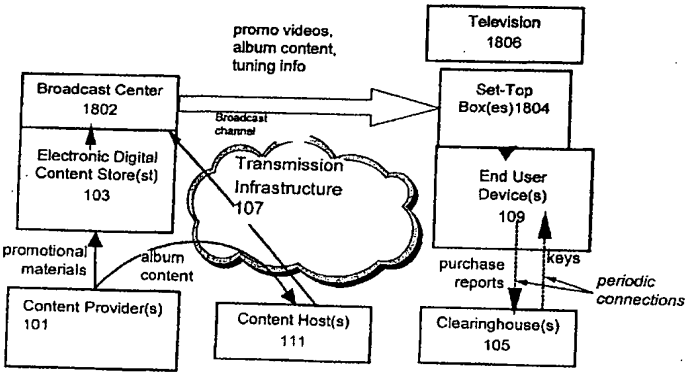


FIG. 18

EP 1 107 137 A2

can remove the ability of the retail stores from differentiating themselves from each other and differentiate themselves from the content owners, especially on the Web. Therefore a need exists to provide retailers of electronic content such as pictures, games, music, programs and videos a way to differentiate themselves from each other and the content owners when selling music through electronic distribution.

[0007] Content owners prepare their digital content for electronic distribution through distribution sites such as electronic stores. Electronic stores on the Internet, or through other online services, want to differentiate themselves from each other by their product offerings and product promotions. A traditional store, i.e. - the non-electronic, non-online analogs to electronic stores - use product promotions, product sales, product samples, liberal return policies and other promotional programs to differentiate themselves from their competitors. However, in the online world where the content providers impose usage conditions on the digital content, the ability of electronic stores to differentiate themselves may be severely limited. Moreover, even if the usage conditions can be changed, electronic stores are faced with the difficult task of processing the metadata associated with the digital content from the content providers to promote and sell products electronically. Electronic stores need to manage several requirements when processing the metadata. First, the electronic store is required to receive the metadata associated with the digital content from the content providers. Many times, parts of this metadata may be sent encrypted, so the content provider must create a mechanism to decrypt the encrypted content. Second, the electronic store may wish to preview metadata from the content provider either before the content is received from the content provider or after the content is received by the electronic store, in order to assist with product marketing, product positioning and other promotional considerations for the content. Third, the electronic store is required to extract certain metadata used for promotional materials such as graphics and artist information. Often, this promotional material is used directly by the electronic store in its online promotions. Fourth, the electronic stores may wish to differentiate themselves from one another by modifying some of the permitted usage conditions to create different offerings of the digital content. Fifth, the electronic store may have to insert or alter certain addresses, such as URLs, in the metadata to direct payment reconciliation to an account reconciliation house automatically by the purchaser without the need to go through the electronic store for payment clearance. Sixth, the electronic store may need to create licenses for the permitted use of the copyrighted digital content that match usage conditions. For example, the license may grant the permission to make a limited number of copies of the digital content. A license is needed to reflect the terms and conditions of the permission granted.

[0008] In light of all these requirements, to process the metadata related to the digital content, many electronic stores write customised software programs to handle these requirements. The time, cost and testing needed to create these customised software programs can be large. Accordingly, a need exists to provide a solution to these requirements.

[0009] Still, another reason owners of digital content have been slow to embrace electronic distribution is the difficulty in preparing content for electronic distribution. Today, many providers of content have thousands or even tens of thousands of titles in their portfolio. In a music example, it is not unusual for a content owner to have a single master sound recording available on several different formats simultaneously (e.g. CD, tape and MiniDisc). In addition, a single format can have a master sound recording re-mastered or re-mixed for a specific distribution channel. As an example, the mixing for broadcast radio may be different than the mixing for a dance club sound track, which may be different than a generally available consumer CD. Inventorying and keeping track of these different mixes can be burdensome. Moreover, many owners of master recordings often times re-issue old recordings in various subsequent collections, such as "The Best Of", or in compilations for musical sound tracks to movies and other collections or compilations. As more content is offered digitally, the need to re-mix and encode the content for electronic distribution grows. Many times providers need to use old recording formats as guides to select the correct master sound recordings and have these sound recordings reprocessed and encoded for release for electronic distribution. This may be especially true for content providers that wish to use their old formats to assist them in re-releasing the old sound recording for electronic distribution. Providers will look through databases to match up titles, artists and sound recordings to set the encoding parameters. This process of manually searching databases for recording portfolios is not without its shortcomings. One shortcoming is the need to have an operator manually search a database and set the processing parameters appropriately. Another shortcoming is the possibility of operator transcription error in selecting data from a database. Accordingly, a need exists to provide content providers a method to automatically retrieve associated data and master recordings for content such as audio.

[0010] Content owners prepare their digital content for electronic distribution through a process known as encoding. Encoding involves taking the content, digitising it, if the content is presented in an analog format, and compressing it. The process of compressing allows the digital content to be transferred over networks and stored on recordable medium more efficiently because the amount of data transmitted or stored is reduced. However, compression is not without its shortcomings. Most compression involves the loss of some information, and is called lossy compression. Content providers must make decisions on what compression algorithm to use and the compression level required. For example, in music, the digital content or song may have very different characteristics depending on the genre of the music. The compression algorithm and compression level selected for one genre may not be the optimal choice for another genre of music. Content providers may find certain combinations of compression algorithms and compression levels work

metadata; receiving data from a second web broadcast channel, the data selected from the promotional metadata, and wherein the data has been previously encrypted using a first encrypting key; and receiving the first decrypting key via a computer readable medium, the first decrypting key for decrypting at least some of the data received via the second web broadcast channel.

[0017] In another embodiment, a method and system to transmit data securely from a web broadcast centre is disclosed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] FIG. 1 is a block diagram illustrating an over view of a Secure Digital Content Electronic Distribution System according to the present invention.

[0019] FIG. 2 is a block diagram illustrating an example Secure Container (SC) and the associated graphical representations according to the present invention.

[0020] FIG. 3 is a block diagram illustrating an overview of the encryption process for a Secure Container (SC) according to the present invention.

[0021] FIG. 4 is a block diagram illustrating an overview of the de-encryption process for a Secure Container (SC) according to the present invention.

[0022] FIG. 5 is a block diagram illustrating an overview of the layers for the Rights Management Architecture of the Secure Digital Content Distribution System of FIG. 1 according to the present invention.

[0023] FIG. 6 is a block diagram illustrating an overview of the Content Distribution and Licensing Control as it applies to the License Control Layer of FIG. 5.

[0024] FIG. 7 is an illustration of an example user interface for the Work Flow Manager Tool of FIG. 1 according to the present invention.

[0025] FIG. 8 is a block diagram of the major tools, components and processes of the Work Flow Manager corresponding to the user interface in FIG. 7 according to the present invention.

[0026] FIG. 9 is a block diagram illustrating the major tools, components and processes of an Electronic Digital Content Store of FIG. 1 according to the present invention.

[0027] FIG. 10 is a block diagram illustrating the major components and processes of an End-User Device(s) of FIG. 1 according to the present invention.

[0028] FIG. 11 is a flow diagram of a method to calculate an encoding rate factor for the Content Preprocessing and Compression tool of FIG. 8 according to the present invention.

[0029] FIG. 12 is a flow diagram of a method to automatically retrieve additional information for the Automatic Metadata Acquisition Tool of FIG. 8 according to the present invention.

[0030] FIG. 13 is a flow diagram of a method to automatically set the Preprocessing and Compression parameters of the Preprocessing and Compression Tool of FIG. 8 according to the present invention.

[0031] FIG. 14 is an example of user interface screens of the Player Application downloading content to a local library as described in FIG. 15 according to the present invention.

[0032] FIG. 15 is a block diagram illustrating the major components and processes of a Player Application running on End-User Device of FIG. 9 according to the present invention.

[0033] FIG. 16 is an example user interface screens of the Player Application of FIG. 15 according to the present invention.

[0034] FIG. 17 is a flow diagram of an alternate embodiment to automatically retrieve additional information for the Automatic Metadata Acquisition Tool of FIG. 8 according to the present invention.

[0035] FIG. 18 is a high level logical diagram of an alternate embodiment of electronic distribution of digital content using broadcast infrastructure, according to the present invention.

[0036] FIG. 19 is a detailed block diagram of FIG. 18, illustrating an alternate embodiment of electronic distribution of digital content using broadcast infrastructure , according to the present invention.

[0037] FIG. 20 is a block diagram of the packet being broadcast in the alternate embodiment of FIG. 18, according to the present invention.

[0038] FIG. 21 is a flow diagram for a process running on the End User Device for purchasing content over the alternate embodiment of FIG. 18., according to the present invention.

[0039] FIGS. 22-26 are a series of screen shots illustrating the user's purchase on a television using the alternate embodiment of FIG. 18, according to the present invention.

[0040] FIG. 27 is a detailed block diagram of FIG. 18, illustrating an alternate embodiment of electronic distribution of digital content using separate channels in a web broadcasting service, according to the present invention.

[0041] FIG. 28 is a flow diagram for a process running on the End User Device for purchasing content over the alternate embodiment of FIG. 27, according to the present invention.

[0042] FIGS. 29-38 are a series of screen shots illustrating the user's purchase on a television using the alternate

V. SECURE CONTAINER STRUCTURE

[0048]

A. General Structure
B. Rights Management Language Syntax and Semantics
C. Overview of Secure Container Flow and Processing
D. Metadata Secure Container 620 Format
E. Offer Secure Container 641 Format
F. Transaction Secure Container 640 Format
G. Order Secure Container 650 Format
H. License Secure Container 660 Format
I. Content Secure Container Format

VI. SECURE CONTAINER PACKING AND UNPACKING

[0049]

A. Overview
B. Bill of Materials (BOM) Part
C. Key Description Part

VII. CLEARINGHOUSE(S)

[0050]

A. Overview
B. Rights Management Processing
C. Country Specific Parameters
D. Audit Logs and Tracking
E. Reporting of Results
F. Billing and Payment Verification
G. Retransmissions

VIII. CONTENT PROVIDER

[0051]

A. Overview
B. Work Flow Manager

1. Products Awaiting Action/Information Process
2. New Content Request Process
3. Automatic Metadata Acquisition Process
4. Manual Metadata Entry Process
5. Usage Conditions Process
6. Supervised Release Process
7. Metadata SC(s) Creation Process
8. Watermarking Process
9. Preprocessing and Compression Process
10. Content Quality Control Process
11. Encryption Process
12. Content SC(s) Creation Process
13. Final Quality Assurance Process
14. Content Dispersement Process
15. Work Flow Rules

C. Metadata Assimilation and Entry Tool

E. End-User Device(s) 109 in Broadcast Delivery Mode

1. Multi-Tier Digital TV Embodiment
2. Web broadcasting Over Separate Channels Embodiment

I. SECURE DIGITAL CONTENT ELECTRONIC DISTRIBUTION SYSTEM

A. System Overview

[0054] The Secure Digital Content Electronic Distribution System is a technical platform that encompasses the technology, specifications, tools, and software needed for the secure delivery and rights management of Digital Content and digital content-related content to an end-user, client device. The End-User Device(s) include PCS, set top boxes (IRDs), and Internet appliances. These devices may copy the content to external media or portable, consumer devices as permitted by the content proprietors. The term Digital Content or simply Content, refers to information and data stored in a digital format including: pictures, movies, videos, music, programs, multimedia and games.

[0055] The technical platform specifies how Digital Content is prepared, securely distributed through point-to-point and broadcast infrastructures (such as cable, Internet, satellite, and wireless) licensed to End-User Device(s), and protected against unauthorised copying or playing. In addition, the architecture of the technical platform allows for the integration and migration of various technologies such as Watermarking, compression/encoding, encryption, and other security algorithms as they evolve over time.

[0056] The base components of the Secure Digital Content Electronic Distribution System are: (1) rights management for the protection of ownership rights of the content proprietor; (2) transaction metering for immediate and accurate compensation; and (3) an open and well-documented architecture that enables Content Provider(s) to prepare content and permit its secure delivery over multiple network infrastructures for playback on any standard compliant player.

1. Rights Management

[0057] Rights management in the Secure Digital Content Electronic Distribution System is implemented through a set of functions distributed among the operating components of the system. Its primary functions include: licensing authorisation and control so that content is unlocked only by authorised intermediate or End-User(s) that have secured a license; and control and enforcement of content usage according to the conditions of purchase or license, such as permitted number of copies, number of plays, and the time interval or term the license may be valid. A secondary function of rights management is to enable a means to identify the origin of unauthorised copies of content to combat piracy.

[0058] Licensing authorisation and control are implemented through the use of a ClearingHouse(s) entity and Secure Container (SC) technology. The ClearingHouse(s) provides licensing authorisation by enabling intermediate or End-User(s) to unlock content after verification of a successful completion of a licensing transaction. Secure Containers are used to distribute encrypted content and information among the system components. A SC is a cryptographic carrier of information or content that uses encryption, digital signatures, and digital certificates to provide protection against unauthorised interception or modification of electronic information and content. It also allows for the verification of the authenticity and integrity of the Digital Content. The advantage of these rights management functions is that the electronic Digital Content distribution infrastructure does not have to be secure or trusted. Therefore allowing transmission over network infrastructures such as the Web and Internet. This is due to the fact that the Content is encrypted within Secure Containers and its storage and distribution are separate from the control of its unlocking and use. Only users who have decryption keys can unlock the encrypted Content, and the ClearingHouse(s) releases decryption keys only for authorised and appropriate usage requests. The ClearingHouse(s) will not clear bogus requests from unknown or unauthorised parties or requests that do not comply with the content's usage conditions as set by the content proprietors. In addition, if the SC is tampered with during its transmission, the software in the ClearingHouse (s) determines that the Content in a SC is corrupted or falsified and repudiate the transaction.

[0059] The control of Content usage is enabled through the End-User Player Application 195 running on an End-User Device(s). The application embeds a digital code in every copy of the Content that defines the allowable number of secondary copies and play backs. Digital Watermarking technology is used to generate the digital code, to keep it hidden from other End-User Player Application 195, and to make it resistant to alteration attempts. In an alternate embodiment, the digital code is just kept as part of the usage conditions associated with the Content 113. When the Digital Content 113 is accessed in a compliant End-User Device(s), the End-User Player Application 195 reads the watermark to check the use restrictions and updates the watermark as required. If the requested use of the content does not comply with the usage conditions, e.g., the number of copies has been exhausted, the End-User Device(s) will not perform the request.

Provider(s) 101 include Sony, Time-Warner, MTV, IBM, Microsoft, Turner, Fox and others.

[0068] Content Provider(s) 101 use tools provided as part of the Secure Digital Content Electronic Distribution System 100 in order to prepare their Content 113 and related data for distribution. A Work Flow Manager Tool 154 schedules Content 113 to be processed and tracks the Content 113 as it flows through the various steps of Content 113 preparation and packaging to maintain high quality assurance. The term metadata is used throughout this document to mean data related to the Content 113 and in this embodiment does not include the Content 113 itself. As an example, metadata for a song may be a song title or song credits but not the sound recording of the song. The Content 113 would contain the sound recording. A Metadata Assimilation and Entry Tool 161 is used to extract metadata from the Content Provider (s)' Database 160 or data provided by the Content Provider(s) in a prescribed format (for a music example the Content 113 information such as CD title, artist name, song title, CD artwork, and more) and to package it for electronic distribution. The Metadata Assimilation and Entry Tool 161 is also used to enter the Usage Conditions for the Content 113. The data in Usage Conditions can include copy restriction rules, the wholesale price, and any business rules deemed necessary. A Watermarking Tool is used to hide data in the Content 113 that identifies the content owner, the processing date, and other relevant data. For an embodiment where the Content 113 is audio, an audio preprocessor tool is used to adjust the dynamics and/or equalise the Content 113 or other audio for optimum compression quality, compress the Content 113 to the desired compression levels, and encrypt the Content 113. These can be adapted to follow technical advances in digital content compression/encoding, encryption, and formatting methods, allowing the Content Provider (s) 101 to utilise best tools as they evolve over time in the marketplace.

[0069] The encrypted Content 113, digital content-related data or metadata, and encrypted keys are packed in SCs (described below) by the SC Packer Tool and stored in a content hosting site and/or promotional web site for electronic distribution. The content hosting site can reside at the Content Provider(s) 101 or in multiple locations, including Electronic Digital Content Store(s) 103 and Intermediate Market Partners (not shown) facilities. Since both the Content 113 and the Keys (described below) are encrypted and packed in SCs, Electronic Digital Content Store(s) 103 or any other hosting agent can not directly access decrypted Content 113 without clearance from the ClearingHouse(s) and notification to the Content Provider(s) 101.

2. Electronic Digital Content Store(s) 103

[0070] Electronic Digital Content Store(s) 103 are the entities who market the Content 113 through a wide variety of services or applications, such as Content 113 theme programming or electronic merchandising of Content 113. Electronic Digital Content Store(s) 103 manage the design, development, business operations, settlements, merchandising, marketing, and sales of their services. Example online Electronic Digital Content Store(s) 103 are Web sites that provide electronic downloads of software.

[0071] Within their services, Electronic Digital Content Store(s) 103 implement certain functions of the Secure Digital Content Electronic Distribution System 100. Electronic Digital Content Store(s) 103 aggregate information from the Content Provider(s) 101, pack content and metadata in additional SCs, and deliver those SCs to consumers or businesses as part of a service or application. Electronic Digital Content Store(s) 103 use tools provided by the Secure Digital Content Electronic Distribution System 100 to assist with: metadata extraction, secondary usage conditions, SC packaging, and tracking of electronic content transactions. The secondary usage conditions data can include retail business offers such as Content 113 purchase price, pay-per-listen price, copy authorisation and target device types, or timed-availability restrictions.

[0072] Once an Electronic Digital Content Store(s) 103 completes a valid request for electronic Content 113 from an End-User(s), the Electronic Digital Content Store(s) 103 is responsible for authorising the ClearingHouse(s) 105 to release the decryption key for the Content 113 to the customer. The Electronic Digital Content Store(s) also authorises the download of the SC containing the Content 113. The Electronic Digital Content Store(s) may elect to host the SCs containing the Digital Content at its local site and/or utilise the hosting and distribution facilities of another Content hosting site.

[0073] The Electronic Digital Content Store(s) can provide customer service for any questions or problems that an End-User(s) may have using the Secure Digital Content Electronic Distribution System 100, or the Electronic Digital Content Store(s) 103 may contract their customer service support to the ClearingHouse(s) 105.

3. Intermediate Market Partners (not shown)

[0074] In an alternate embodiment, the Secure Digital Content Electronic Distribution System 100 can be used to provide Content 113 securely to other businesses called Intermediate Market Partners. These partners may include digital content-related companies offering a non-electronic service, such as televisions stations or video clubs, radio stations or record clubs, that distribute Content 113. These Partners may also include other trusted parties who handle material as part of making or marketing sound recordings, such as record studios, replicators, and producers. These

C. System Uses

[0081] The Secure Digital Content Electronic Distribution System 100 enables the secure delivery of high-quality, electronic copies of Content 113 to End-User Device(s) 109, whether consumer or business, and to regulate and track usage of the Content 113.

[0082] The Secure Digital Content Electronic Distribution System 100 could be deployed in a variety of consumer and business-to-business services using both new and existing distribution channels. Each particular service could use a different financial model that can be enforced through the rights management features of the Secure Digital Content Electronic Distribution System 100. Models such as wholesale or retail purchase, pay-per-listen usage, subscription services, copy/no-copy restrictions, or redistribution could be implemented through the rights management of the ClearingHouse(s) 105 and the End-User Player Application 195 copy protection features.

[0083] The Secure Digital Content Electronic Distribution System 100 allows Electronic Digital Content Store(s) 103 and Intermediate Market Partners a great deal of flexibility in creating services that sell Content 113. At the same time it provides Content Provider(s) 101 a level of assurance that their digital assets are protected and metered so that they can receive appropriate compensation for the licensing of Content 113.

II. CRYPTOGRAPHY CONCEPTS AND THEIR APPLICATION TO THE SECURE DIGITAL CONTENT ELECTRONIC DISTRIBUTION SYSTEM

[0084] License Control in the Secure Digital Content Electronic Distribution System 100 is based on the use of cryptography. This section introduces basic cryptography technologies of the present invention. The use of public key encryption, symmetric key encryption, digital signatures, digital watermarks and digital certificates is known.

A. Symmetric Algorithms

[0085] In the Secure Digital Content Electronic Distribution System 100 the Content Provider(s) 101 encrypts the content using symmetric algorithms. They are called symmetric algorithms because the same key is used to encrypt and decrypt data. The data sender and the message recipient must share the key. The shared key is referred to here as the symmetric key. The Secure Digital Content Electronic Distribution System 100 architecture is independent of the specific symmetric algorithm selected for a particular implementation.

[0086] Common symmetric algorithms are DES, RC2 and RC4. Both DES and RC2 are block cipher. A block cipher encrypts the data using a block of data bits at a time. DES is an official US government encryption standard, has a 64-bit block size, and uses a 56-bit key. Triple-DES is commonly used to increase the security achieved with simple DES. RSA Data Security designed RC2. RC2 uses a variable-key-size cipher and has a block size of 64 bits. RC4, also designed by RSA Data Security, is a variable-key-size stream cipher. A stream cipher operates on a single data bit at a time. RSA Data Security claims that eight to sixteen machine operations are required for RC4 per output byte.

[0087] IBM designed a fast algorithm called SEAL. SEAL is a stream algorithm that uses a variable-length key and that has been optimised for 32-bit processors. SEAL requires about five elementary machine instructions per data byte. A 50 MHZ, 486-based computer runs the SEAL code at 7.2 megabytes/second if the 160-bit key used has already been preprocessed into internal tables.

[0088] Microsoft reports results of encryption performance benchmark in its Overview of CryptoAPI document. These results were obtained by an application using Microsoft's CryptoAPI, running on a 120-MHZ, Pentium-based computer with Windows NT 4.0.

Cipher	Key Size	Key Setup Time	Encryption Speed
DES	56	460	1,138,519
RC2	40	40	286,888
RC4	40	151	2,377,723

B. Public Key Algorithms

[0089] In the Secure Digital Content Electronic Distribution System 100, symmetric keys and other small data pieces are encrypted using public keys. Public key algorithms use two keys. The two keys are mathematically related so that data encrypted with one key can only be decrypted with the other key. The owner of the keys keeps one key private (private key) and publicly distributes the second key (public key).

[0090] To secure the transmission of a confidential message using a public key algorithm, one must use the recipient's

public key. PV inside the handle indicates that it is a private key. Diamond shape is an End-User Digital Signature 202. The initials indicate which private key was used to create the signature thus in EU is the End-User(s) digital signature from table below. Symmetric key 203 is used to encrypt content. An encrypted symmetric key object 204 comprising a symmetric key 203 encrypted with a PB of CLRNGH. The key on the top border of the rectangle is the key used in the encryption of the object. The symbol or text inside the rectangle indicates the encrypted object (a symmetric key in this case). Another encrypted object, in this example a Transaction ID encrypted object 205 is shown. And Usage Conditions 206 for content licensing management as described below. The SC(s) 200 comprises Usage Conditions 206, Transaction ID encrypted object 205, an Application ID encrypted object 207, and encrypted symmetric key object 204, all signed with an End-User Digital Signature 202.

[0101] The table below shows the initials that identify the signer of SC(s).

Initial	Component
CP	Content Provider(s) 101
MS	Electronic Digital Content 103
HS	Content Hosting Site(s) 111
EU	End-User Device(s) 109
CH	Clearinghouse(s) 105
CA	certification authority(ies)

F. Example of a Secure Container Encryption

[0102] The tables and diagrams below provide an overview of the encryption and decryption process used to create and recover information from SC(s). The SC(s) that is created and decrypted in this process overview is a general SC (s). It does not represent any of the specific SC(s) types used for rights management in the Secure Digital Content Electronic Distribution System 100. The process consists of the steps described in FIG.3 for encryption process.

Process Flow for Encryption Process of FIG.3

[0103]

Step	Process
301	Sender generates a random symmetric key and uses it to encrypt the content.
302	Sender runs the encrypted content through a hash algorithm to produce the content digest.
303	Sender encrypts the symmetric key using the recipient's public key. PB RECPNT refers to the recipient's public key.
304	Sender runs the encrypted symmetric key through the same hash algorithm used in step2 to produce the symmetric key digest.
305	Sender runs the concatenation of the content digest and symmetric key digest through the same hash algorithm used in step2 to produce the SC(s) digest.
306	Sender encrypts the SC(s) digest with the sender's private key to produce the digital signature for the SC (s). PV SENDER refers to the sender's private key.
307B	Sender creates a SC(s) file that includes the encrypted content, encrypted symmetric key, content digest, symmetric key digest, sender's certificate, and SC(s) signature.
307A	Sender must have obtained the certificate from a certification authority prior to initiating secure communications. The certification authority includes in the certificate the sender's public key, the sender's name and signs it. PV CAUTHR refers to the certifications authority's private key. Sender transmits the SC (s) to the recipient.

Step	Process
121	A uncompressed PCM audio file is provided as Content 113 by the Content Provider(s) 101. Its filename is input into the Work Flow Manager 154 Tool along with the Content Provider(s)' 101 unique identifier for the Content 113.
122	Metadata is captured from the Content Provider(s)' Database 160 by the Content Information Processing Subsystem using the Content Provider(s)' 101 unique identifier for the Content 113 and information provided by the Database Mapping Template.
123	The Work Flow Manager Tool 154 is used to direct the content flow through the acquisition and preparation process at the Content Provider(s) 101. It can also be used to track the status of any piece of content in the system at any time.
124	The Usage Conditions for the Content 113 are entered into the Content Information Processing Subsystem, this can be done either manually or automatically. This data includes copy restriction rules and any other business rules deemed necessary. All of the metadata entry can occur in parallel with the Audio Processing for the data.
125	The Watermarking Tool is used to hide data in the Content 113 that the Content Provider(s) 101 deems necessary to identify the content. This could include when it was captured, where it came from (this Content Provider(s) 101), or any other information specified by the Content Provider(s) 101. • The Content Processing Tool 125 performs equalisation, dynamics adjustments and re-sampling to the Content 113 as necessary for the different compression levels supported. • The Content 113 is compressed using the Content Processing Tool 125 to the desired compression levels. The Content 113 can then be played back to verify that the compression produces the required level of Content 113 quality. If necessary the equalisation, dynamics adjustments, compression and playback quality checks can be performed as many times as desired. • The Content 113 and a subset of its metadata is encrypted Symmetric Key by the SC Packer. This tool then encrypts the key using the Public Key of the ClearingHouse(s) 105 to produce an Encrypted Symmetric Key. This key can be transmitted anywhere without comprising the security of the Content 113 since the only entity that can decrypt it is the ClearingHouse(s) 105.
126	The Encrypted Symmetric Key, metadata and other information about the Content 113 is then packed into a Metadata SC by the SC Packer Tool 152.
127	The encrypted Content 113 and metadata are then packed into a Content SC. At this point the processing on the Content 113 and metadata is complete.
128	The Metadata SC(s) is then sent to the Content Promotions Web Site 156 using the Content Disbursement Tool (not shown).
129	The Content Disbursement Tool sends the Content SC(s) to the Content Hosting Site(s) 111. The Content Hosting Site(s) can reside at the Content Provider(s) 101, the ClearingHouse(s) 105 or a special location dedicated for Content Hosting. The URL for this site is part of the metadata that was added to the Metadata SC.
130	The Content Promotions Web Site 156 notifies Electronic Digital Content Store(s) 103 of new Content 113 that is added to the System 100.
131	Using the Content Acquisition Tool, Electronic Digital Content Store(s) 103 then download the Metadata SCs that correspond to the Content 113 they wish to sell.
132	The Electronic Digital Content Store(s) 103 will use the Content Acquisition Tool to pull out any data from the Metadata SC(s) that they want to use to promote the Content 113 on their Web Site. Access to portions of this metadata can be secured and charged for if desired.
133	The Usage Conditions for the Content 113, specific to this Electronic Digital Content Store(s) 103, are entered using the Content Acquisition Tool. These Usage Conditions include the retail prices and copy/play restrictions for the different compression levels of the Content 113.
134	The Electronic Digital Content Store(s) 103 specific Usage Conditions and the original Metadata SC(s) are packed into an Offer SC by the SC Packer Tool.
135	After the Electronic Digital Content Store(s) 103 Web Site is updated, the Content 113 is available to End-User(s) surfing the Web.

- the Content 113 originates from a rightful content owner and is distributed by a licensed distributor, e.g. Electronic Digital Content Store(s) 103;
- the Digital Content purchaser has a properly licensed application;
- the distributor is paid by the purchaser before a copy of the Content 113 is made available to the purchaser or End-User(s); and
- a record of the transaction is kept for reporting purposes.

[0110] The Content Identification Layer 503 allows for the verification of the copyright and the identity of the content purchaser. The content's copyright information and identity of the content purchaser enables the source tracking of any, authorised or not, copy of the Content 113. Thus, the Content Identification Layer 503 provides a means to combat piracy.

[0111] The Content Usage Control Layer 505 ensures that the copy of the Content 113 is used in the purchaser's device according to the Store Usage Conditions 519. The Store Usage Conditions 519 may specify the number of plays and local copies allowed for the Content 113, and whether or not the Content 113 may be recorded to an external portable device. The functions in the Content Usage Control Layer 505 keep track of the content's copy/play usage and update the copy/play status.

[0112] The Content Formatting Layer 507 allows for the format conversion of the Content 113 from its native representation in the content owner's facilities into a form that is consistent with the service features and distribution means of the Secure Digital Content Electronic Distribution System 100. The conversion processing may include compression encoding and its associated preprocessing, such as frequency equalisation and amplitude dynamic adjustment. For Content 113 which is audio, at the purchaser's side, the received Content 113 also needs to be processed to achieve a format appropriate for playback or transfer to a portable device.

B. Function Partitioning and Flows

[0113] The Rights Management Architectural Model is shown in FIG.5 and this illustrates the mapping of the architectural layers to the operating components making up the Secure Digital Content Electronic Distribution System 100 and the key functions in each layer.

1. Content Formatting Layer 507

[0114] The general functions associated with the Content Formatting Layer 507 are Content Preprocessing 502 and Compression 511 at the Content Provider(s) 101, and Content De-scrambling 513 and Decompression 515 at the End-User Device(s) 109. The need for preprocessing and the examples of specific functions were mentioned above. Content Compression 511 is used to reduce the file size of the Content 113 and its transmission time. Any compression algorithm appropriate for the type of Content 113 and transmission medium can be used in the Secure Digital Content Electronic Distribution System 100. For music, MPEG ½/4, Dolby AC-2 and AC-3, Sony Adaptive Transform Coding (ATRAC), and low-bit rate algorithms are some of the typically used compression algorithms. The Content 113 is stored in the End-User Device(s) 109 in compressed form to reduce the storage size requirement. It is decompressed during active playback. De-scrambling is also performed during active playback. The purpose and type of scrambling will be described later during the discussion of the Content Usage Control Layer 505.

2. Content Usage Control Layer 505

[0115] The Content Usage Control Layer 505 permits the specification and enforcement of the conditions or restrictions imposed on the use of Content 113 use at the End-User Device(s) 109. The conditions may specify the number of plays allowed for the Content 113, whether or not a secondary copy of the Content 113 is allowed, the number of secondary copies, and whether or not the Content 113 may be copied to an external portable device. The Content Provider(s) 101 sets the allowable Usage Conditions 517 and transmits them to the Electronic Digital Content Store (s) 103 in a SC (see the License Control Layer 501 section). The Electronic Digital Content Store(s) 103 can add to or narrow the Usage Conditions 517 as long as it doesn't invalidate the original conditions set by the Content Provider (s) 101. The Electronic Digital Content Store(s) 103 then transmits all Store Usage Conditions 519 (in a SC) to the End-User Device(s) 109 and the ClearingHouse(s) 105. The ClearingHouse(s) 105 perform Usage Conditions Validation 521 before authorising the Content 113 release to an End-User Device(s) 109.

[0116] The enforcement of the content Usage Conditions 517 is performed by the Content Usage Control Layer 505 in the End-User Device(s) 109. First, upon reception of the Content 113 copy from the Content Identification Layer 503 in the End-User Device(s) 109 marks the Content 113 with a Copy/Play Code 523 representing the initial copy/play permission. Second, the Player Application 195 cryptographically scrambles the Content 113 before storing it in the

purchase commercial transaction between the End-User Device(s) 109 and the Electronic Digital Content Store(s) 103 is based on standard Internet Web protocols. As part of the Web-based interaction, the End-User(s) makes the selection of the Content 113 to purchase, provides personal and financial information, and agrees to the conditions of purchase. The Electronic Digital Content Store(s) 103 could obtain payment authorisation from an acquirer institution using a protocol such as SET.

[0124] It is also assumed in FIG.6 that the Electronic Digital Content Store(s) 103 has downloaded the End-User Player Application 195 to an End-User Device(s) 109 based on standard Web protocols. The architecture requires that the Electronic Digital Content Store(s) 103 assigns a unique application ID to the downloaded Player Application 195 and that the End-User Device(s) 109 stores it for later application license verification (see below).

[0125] The overall licensing flow starts at the Content Provider(s) 101. The Content Provider(s) 101 encrypts the Content 113 using an encryption symmetric key locally generated, and encrypts the Symmetric Key 623 using the Clearinghouse's 105 public key 621. In an alternate embodiment, the symmetric key instead of being locally generated my be sent to the Content Provider(s) 101 from the ClearingHouse(s) 105. The Content Provider(s) 101 creates a Content SC(s) 630 around the encrypted Content 113, and a Metadata SC(s) 620 around the encrypted Symmetric Key 623, Store Usage Conditions 519, and other Content 113 associated information. There is one Metadata SC(s) 620 and one Content SC(s) 630 for every Content 113 object. The Content 113 object may be a compression level one same song or the Content 113 object may be each song on the album or the Content 113 object may be the entire album. For each Content 113 object, the Metadata SC(s) 620 also carries the Store Usage Conditions 519 associated with the Content Usage Control Layer 505.

[0126] The Content Provider(s) 101 distributes the Metadata SC(s) 620 to one or more Electronic Digital Content Store(s) 103 (step601) and the Content SC(s) 630 to one or more Content Hosting Sites (step602). Each Electronic Digital Content Store(s) 103, in turn creates an Offer SC(s) 641. The Offer SC(s) 641 typically carries much of the same information as the Metadata SC(s) 620, including the Digital Signature 624 of the Content Provider(s) 101 and the Certificate (not shown of the Content Provider(s) 101. As mentioned above, the Electronic Digital Content Store (s) 103 can add to or narrow the Store Usage Conditions 519 (handled by the Control Usage Control Layer) initially defined by the Content Provider(s) 101. Optionally, the Content SC(s) 630 and/or the Metadata SC(s) 620 is signed with a Digital Signature 624 of the Content Provider(s) 101.

[0127] After the completion of the Content-purchase transaction between the End-User Device(s) 109 and the Electronic Digital Content Store(s) 103 (step603), the Electronic Digital Content Store(s) 103 creates and transfers to the End-User Device(s) 109 a Transaction SC(s) 640 (step604). The Transaction SC(s) 640 includes a unique Transaction ID 535, the purchaser's name (i.e. End-User(s)') (not shown), the Public Key 661 of the End-User Device(s) 109, and the Offer SC(s) 641 associated with the purchased Content 113. Transaction Data 642 in FIG.6 represents both the Transaction ID 535 and the End-User(s) name (not shown). The Transaction Data 642 is encrypted with the Public Key 621 of the ClearingHouse(s) 105. Optionally, the Transaction SC(s) 640 is signed with a Digital Signature 643 of the Electronic Digital Content Store(s) 103.

[0128] Upon reception of the Transaction SC(s) 640 (and the Offer SC(s) 641 included in it), the End-User Player Application 195 running on End-User Device(s) 109 solicits license authorisation from the ClearingHouse(s) 105 by means of an Order SC(s) 650 (step605). The Order SC(s) 650 includes the encrypted Symmetric Key 623 and Store Usage Conditions 519 from the Offer SC(s) 641, the encrypted Transaction Data 642 from the Transaction SC(s) 640, and the encrypted Application ID 551 from the End-User Device(s) 109. In another embodiment, the Order SC(s) 650 is signed with a Digital Signature 652 of the End-User Device(s) 109.

[0129] Upon reception of the Order SC(s) 650 from the End-User Device(s) 109, the ClearingHouse(s) 105 verifies:

1. that the Electronic Digital Content Store(s) 103 has authorisation from the Secure Digital Content Electronic Distribution System 100 (exists in the Database 160 of the ClearingHouse(s) 105);
2. that the Order SC(s) 650 has not been altered;
3. that the Transaction Data 642 and Symmetric Key 623 are complete and authentic;
4. that the electronic Store Usage Conditions 519 purchased by the End-User Device(s) 109 are consistent with those Usage Conditions 517 set by the Content Provider(s) 101; and
5. that the Application ID 551 has a valid structure and that it was provided by an authorised Electronic Digital Content Store(s) 103. If the verifications are successful, the ClearingHouse(s) 105 decrypts the Symmetric Key 623 and the Transaction Data 642 and builds and transfers the License SC(s) 660 to the End-User Device(s) 109 (step606). The License SC(s) 660 carries the Symmetric Key 623 and the Transaction Data 642, both encrypted using the Public Key 661 of the End-User Device(s) 109. If any verification is not successful, the ClearingHouse (s) 105 denies the license to the End-User Device(s) 109 and informs the End-User Device(s) 109. The ClearingHouse(s) 105 also immediately informs the Electronic Digital Content Store(s) 103 of this verification failure. In an alternate embodiment, the ClearingHouse(s) 105 signs the License SC(s) 660 with its Digital Signature 663.

identifier of the symmetric key that was used to encrypt the encrypted part.

[0137] If the SC(s) does not contain any encrypted parts, then there is no Key Description part.

B. Rights Management Language Syntax and Semantics

[0138] The Rights Management Language consists of parameters that can be assigned values to define restrictions on the use of the Content 113 by an End-User(s) after the Content 113 purchase. The restrictions on the use of the Content 113 is the Usage Conditions 517. Each Content Provider(s) 101 specifies the Usage Conditions 517 for each of its Content 113 items. Electronic Digital Content Store(s) 103 interpret the Usage Conditions 517 in Metadata SC (s) 620 and use the information to provide select options they wish to offer their customers as well as add retail purchase information for the Content 113. After an End-User(s) has selected a Content 113 item for purchase, the End-User Device(s) 109 requests authorisation for the Content 113 based on Store Usage Conditions 519. Before the Clearing-House(s) 105 sends a License SC(s) 660 to the End-User(s), the ClearingHouse(s) 105 verifies that the Store Usage Conditions 519 being requested are in agreement with the allowable Usage Conditions 517 that were specified by the Content Provider(s) 101 in the Metadata SC(s) 620.

[0139] When an End-User Device(s) 109 receives the Content 113 that was purchased, the Store Usage Conditions 519 are encoded into that Content 113 using the Watermarking Tool or encoded in the securely stored Usage Conditions 519. The End-User Player Application 195 running on End-User Device(s) 109 insures that the Store Usage Conditions 519 that were encoded into the Content 113 are enforced.

[0140] The following are examples of Store Usage Conditions 519 for an embodiment where the Content 113 is music:

- Song is recordable.
- Song can be played n number of times.

C. Overview of Secure Container Flow and Processing

[0141] Metadata SC(s) 620 are built by Content Provider(s) 101 and are used to define Content 113 items such as songs. The Content 113 itself is not included in these SC(s) because the size of the Content 113 is typically too large for Electronic Digital Content Store(s) 103 and End-User(s) to efficiently download the containers just for the purpose of accessing the descriptive metadata. Instead, the SC(s) includes an external URL (Uniform Resource Locators) to point to the Content 113. The SC(s) also includes metadata that provides descriptive information about the Content 113 and any other associated data, such as for music, the CD cover art and/or digital audio clips in the case of song Content 113.

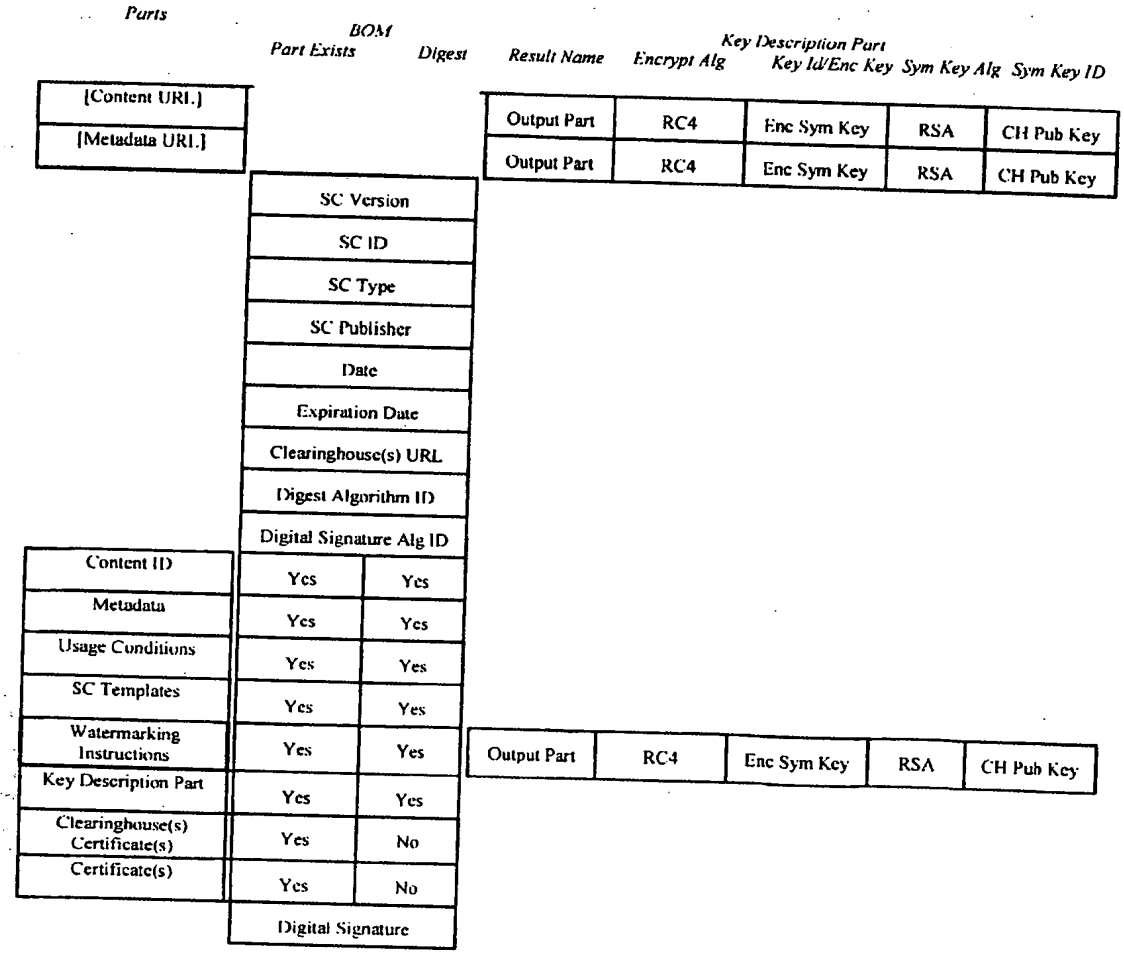
[0142] Electronic Digital Content Store(s) 103 download the Metadata SC(s) 620, for which they are authorised, and build Offer SC(s) 641. In short, an Offer SC(s) 641 consists of some of the parts and the BOM from the Metadata SC (s) 620 along with additional information included by the Electronic Digital Content Store(s) 103. A new BOM for the Offer SC(s) 641 is created when the Offer SC(s) 641 is built. Electronic Digital Content Store(s) 103 also use the Metadata SC(s) 620 by extracting metadata information from them to build HTML pages on their web sites that present descriptions of Content 113 to End-User(s), usually so they can purchase the Content 113.

[0143] The information in the Offer SC(s) 641 that is added by the Electronic Digital Content Store(s) 103 is typically to narrow the selection of Usage Conditions 517 that are specified in the Metadata SC(s) 620 and promotional data such as a graphic image file of the store's logo and a URL to the store's web site. An Offer SC(s) 641 template in the Metadata SC(s) 620 indicates which information can be overridden by the Electronic Digital Content Store(s) 103 in the Offer SC(s) 641 and what, if any, additional information is required by the Electronic Digital Content Store(s) 103 and what parts are retained in the embedded Metadata SC(s) 620.

[0144] Offer SC(s) 641 are included in a Transaction SC(s) 640 when an End-User(s) decides to purchase Content 113 from an Electronic Digital Content Store(s) 103. The Electronic Digital Content Store(s) 103 builds a Transaction SC(s) 640 and includes Offer SC(s) 641 for each Content 113 item being purchased and transmits it to the End-User Device(s) 109. The End-User Device(s) 109 receives the Transaction SC(s) 640 and validates the integrity of the Transaction SC(s) 640 and the included Offer SC(s) 641.

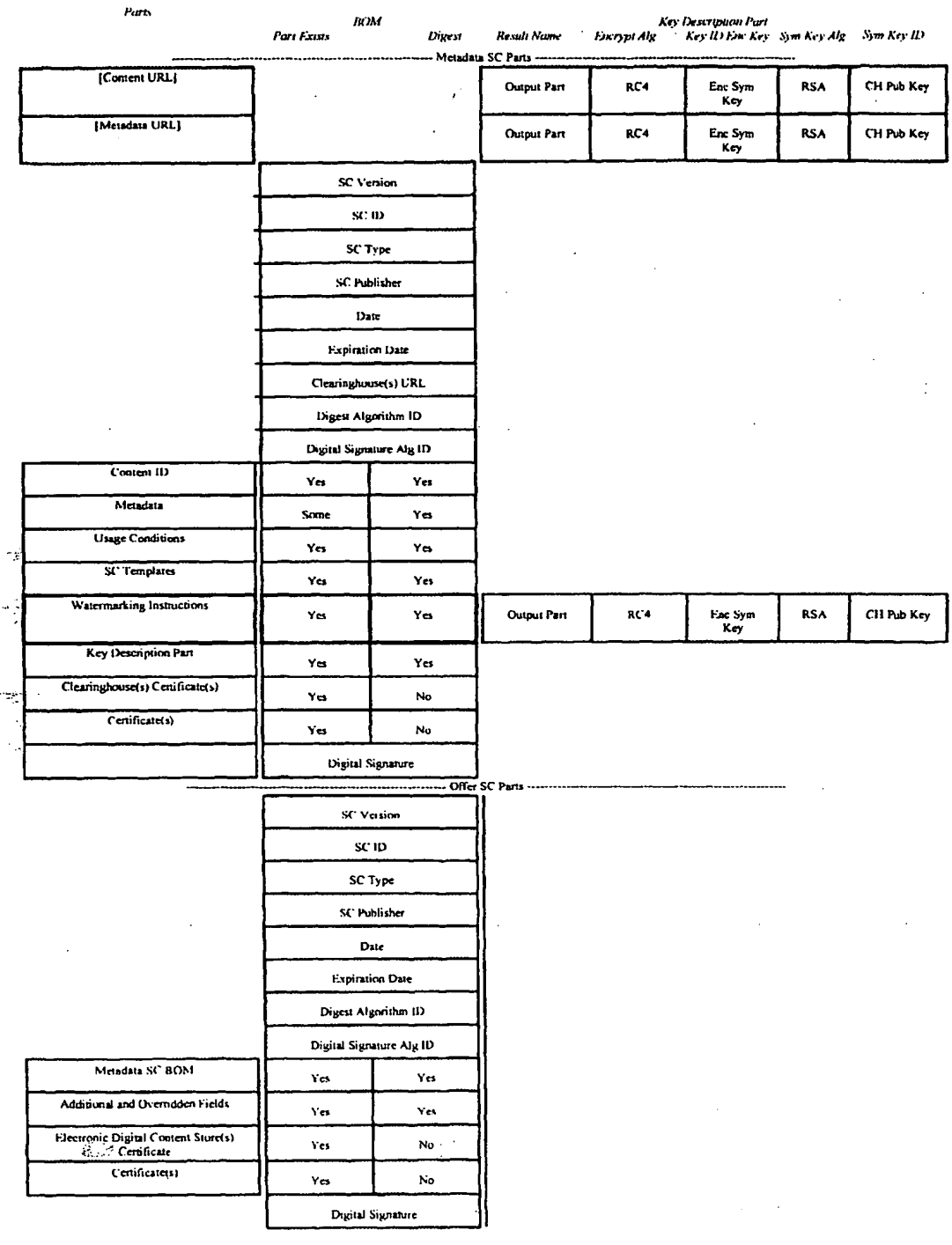
[0145] An Order SC(s) 650 is built by the End-User Device(s) 109 for each Content 113 item being purchased. Information is included from the Offer SC(s) 641, from the Transaction SC(s) 640, and from the configuration files of the End-User Device(s) 109. Order SC(s) 650 are sent to the ClearingHouse(s) 105 one at a time. The ClearingHouse (s) 105 URL where the Order SC(s) 650 is included as one of the records in the BOM for the Metadata SC(s) 620 and included again in the Offer SC(s) 641.

[0146] The ClearingHouse(s) 105 validates and processes Order SC(s) 650 to provide the End-User Device(s) 109 with everything that is required to a License Watermark 527 and access purchased Content 113. One of the functions



[0151] The following describes the terms that are used in the above Metadata SC(s) table:

- [Content URL] - A parameter in a record in the Key Description part. This is a URL that points to the encrypted Content 113 in the Content SC(s) 630 that is associated with this Metadata SC(s) 620. The Metadata SC(s) 620 itself does not contain the encrypted Content 113.
- [Metadata URL] - A parameter in a record in the Key Description part. This is a URL that points to the encrypted metadata in the Content SC(s) 630 that is associated with this Metadata SC(s) 620. The Metadata SC(s) 620 itself does not contain the encrypted metadata.
- Content ID - A part that defines a unique ID assigned to a Content 113 item. There is more than one Content ID included in this part if the Metadata SC(s) 620 references more than one Content 113 item.
- Metadata - Parts that contain information related to a Content 113 item such as the artist name and CD cover art in the case of a song. There may be multiple metadata parts, some of which may be encrypted. The internal structure of the metadata parts is dependent on the type of metadata contained therein.
- Usage Conditions - A part that contains information that describes usage options, rules, and restrictions to be imposed on an End-User(s) for use of the Content 113.
- SC(s) Templates - Parts that define templates that describe the required and optional information for building the Offer, Order, and License SC(s) 660.
- Watermarking Instructions - A part that contains the encrypted instructions and parameters for implementing watermarking in the Content 113. The watermarking instructions may be modified by the ClearingHouse(s) 105 and returned back to the End-User Device(s) 109 within the License SC(s) 660. There is a record in the Key Description



[0153] The following describes the terms that are used in the above Offer SC(s) 641 that were not previously described for another SC(s):

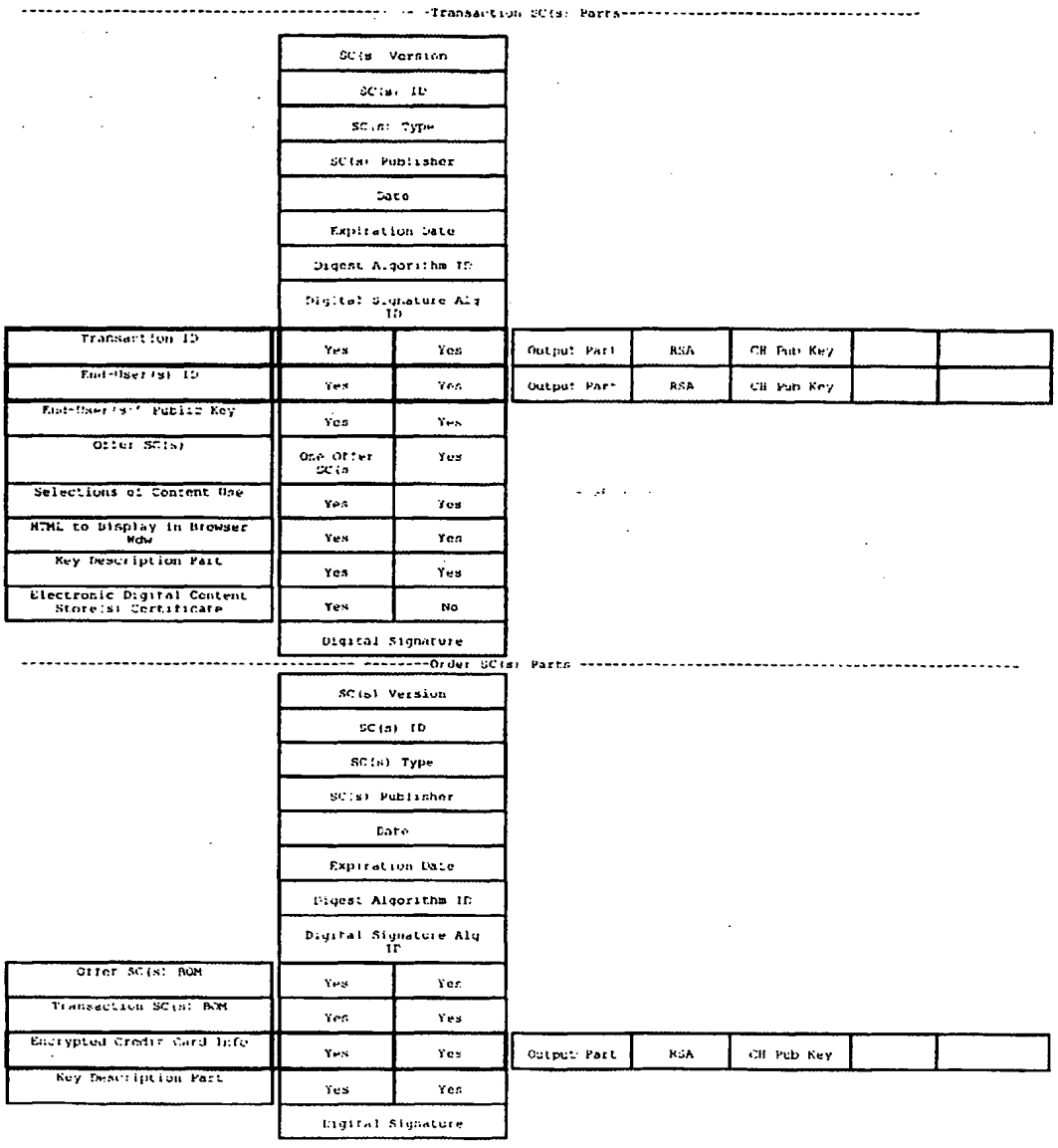
- End-User(s)' Public Key - The End-User(s)' Public Key 661 that is used by the ClearingHouse(s) 105 to re-encrypt the Symmetric Keys 623. The End-User(s)' Public Key 661 is transmitted to the Electronic Digital Content Store (s) 103 during the purchase transaction.
- Offer SC(s) - Offer SC(s) 641 for the Content 113 items that were purchased.
- Selections of Content Use - An array of Usage Conditions for each Content 113 item being purchased by the End-User(s). There is an entry for each Offer SC(s) 641.
- HTML to Display - One or more HTML pages that the End-User Player Application 195 displays in the Internet browser window upon receipt of the Transaction SC(s) 640 or during the interaction between the End-User Device (s) 109 and the ClearingHouse(s) 105.

[0156] When the End-User Device(s) 109 receives a Transaction SC(s) 640, the following steps may be performed to verify the integrity and authenticity of the SC(s):

1. Verify the integrity of the Electronic Digital Content Store(s) 103 certificate using the Public Key 621 of the ClearingHouse(s) 105. The Public Key 621 of the ClearingHouse(s) 105 was stored at the End-User Device(s) 109 after it was received as part of the initialisation of the End-User Player Application 195 during its installation process.
2. Verify the Digital Signature 643 of the SC(s) using the public key from the Electronic Digital Content Store(s) 103 certificate.
3. Verify the hashes of the SC(s) parts.
4. Verify the integrity and authenticity of each Offer SC(s) 641 included in the Transaction SC(s) 640.

G. Order Secure Container 650 Format

[0157] The following table shows the parts that are included in the Order SC(s) 650 as well as its BOM and Key Description parts. These parts either provide information to the ClearingHouse(s) 105 for decryption and verification purposes or is validated by the ClearingHouse(s) 105. The parts and BOM from the Offer SC(s) 641 are also included in the Order SC(s) 650. The Some string in the Part Exists column of the Metadata SC(s) BOM indicates that the some of those parts are not included in the Order SC(s) 650. The BOM from the Metadata SC(s) 620 is also included without any change so that the ClearingHouse(s) 105 can validate the integrity of the Metadata SC(s) 620 and its parts.



The following describes the terms that are used in the above Order SC(s) 650 that were not previously described for another SC(s):

- Transaction SC(s) BOM - The BOM in the original Transaction SC(s) 640. The record in the Order SC(s) 650 BOM includes the digest of the Transaction SC(s) 640 BOM.
- Encrypted Credit Card Info.- Optional encrypted information from the End-User(s) that is used to charge the purchase to a credit card or • debit card. This information is required when the Electronic Digital Content Store(s) 103 that created the Offer SC(s) 641 does not handle the customer billing, in which case the ClearingHouse(s) 105 may handle the billing.

I. Content Secure Container Format

[0160] The following table shows the parts that are included in the Content SC(s) 630 as well as the BOM:

Parts	*BOM*	
	Part Exists	*Digest*
	S(s) Version	
	SC(s) ID	
	SC(s) Type	
	SC(s) Publisher	
	Date	
	Expiration Date	
	Clearinghouse(s) 105 URL	
	Digest Algorithm ID	
	Digital Signature Alg ID	
Content ID	Yes	Yes
Encrypted Content	Yes	Yes
Encrypted Metadata	Yes	Yes
Metadata	Yes	Yes
Certificate(s)	Yes	No
	Digital Signature	

[0161] The following describes the terms used in the above Content SC(s) 630 that were not previously described for another SC(s):

- Encrypted Content - Content 113 that was encrypted by a Content Provider(s) 101 using a Symmetric Key 623.
- Encrypted Metadata - Metadata associated with the Content 113 that was encrypted by a Content Provider(s) 101 using a Symmetric Key 623.

[0162] There is no Key Description part included in the Content SC(s) 630 since the keys required to decrypt the encrypted parts are in the License SC(s) 660 that is built at the ClearingHouse(s) 105.

VI. SECURE CONTAINER PACKING AND UNPACKING

A. Overview

[0163] The SC(s) Packer is a 32-bit Windows' program with an API (Application Programming Interface) that can be called in either a multiple or single step process to create a SC(s) with all of the specified parts. The SC(s) Packer 151, 152, 153 variety of hardware platforms supporting Windows' program at the Content Provider(s) 101, ClearingHouse (s) 105, Electronic Digital Content Store(s) 103 and other sites requiring SC(s) Packing. A BOM and, if necessary, a Key Description part are created and included in the SC(s). A set of packer APIs allows the caller to specify the information required to generate the records in the BOM and Key Description parts and to include parts in the SC(s). Encryption of parts and Symmetric Keys 623 as well as computing the digests and the digital signature is also be performed by the packer. Encryption and digest algorithms that are supported by the packer are included in the packer

The ID property is a unique value that is assigned to this specific SC(s) by the entity that is creating this SC(s). The format of the value is defined in a later version of this document.

T value The T property specifies the type of the SC(s), which should be one of:

ORD - An Order SC(s) 650.
OFF - An Offer SC(s) 641.
LIC - A License SC(s).
TRA - A Transaction SC(s) 640.
MET - A Metadata SC(s) 620.
CON - A Content SC(s) 630.

A value
The A property identifies the author or publisher of the SC(s). Author/publisher identities should be unambiguous and/or registered with the ClearingHouse(s) 105.

D value
The D property identifies the date, and optionally, the time that the SC(s) was created. The value should be of the form yyyy/mm/dd[@hh:mm[:ss[.fsec]][(TZ)]] representing year/month/day@hour:minute:second.decimal-fraction-of-second (time-zone). Optional parts of the value are enclosed in [] characters.

E value
The E property identifies the date, and optionally, the time that the SC(s) expires. The value should be the same form used in the D property that was previously defined. The expiration date/time should be compared, whenever possible, with the date/time at the ClearingHouse(s) 105.

CCURL value
The CCURL property identifies the URL of the ClearingHouse(s) 105. The value should be of the form of a valid external URL.

H value
The H property identifies the algorithm that was used to calculate the message digests for the parts included in the SC(s). An example digest algorithm is MD5.

D A D record is a data or part entry record that contains information that identifies the type of part, the name of the part, the (optional) digest of the part, and an (optional) indication that the part is not included in the SC(s). A - sign immediately after the type identifier is used to indicate that the part is not included in the SC(s). The following are reserved types of data or part records:

K part_name [digest]
Specifies the Key Description part.

W part_name [digest]
Specifies the watermarking instructions part.

C part_name [digest]
Specifies the certificate(s) used to validate the digital signature.

T part_name [digest]
Specifies the Usage Conditions part.

YF part_name [digest]
Specifies the Template part for the Offer SC(s) 641.

YO part_name [digest]
Specifies the Template part for the Order SC(s) 650.

YL part name [digest]
Specifies the Template part for the License SC(s) 660.

ID part_name [digest]
Specifies the ID(s) of the Content 113 of the item(s) of Content 113 being referenced.

CH part_name [digest]
Specifies the ClearingHouse(s) 105 certificate part.

SP part_name [digest] Specifies the Electronic Digital Content Store(s) 103 certificate part.

B part_name [digest]
Specifies a BOM part for another SC(s) that has its parts or a subset of its parts included in this SC(s).

BP part_name sc_part_name [digest]
Specifies a BOM part for another SC(s) that is included as a single part in this SC(s). The sc_part_name parameter is the name of the SC(s) part that is included in this SC(s) and that this BOM part defines. A

process for making the request so long as the two parties come to an agreement. After the digital content label such as a Music Label e.g. Sony, Time-Warner, etc. decides to allow the Electronic Digital Content Store(s) 103 to sell its Content 113, the ClearingHouse(s) 105 is contacted, usually via E-mail, with a request that the Electronic Digital Content Store(s) 103 be added to the Secure Digital Content Electronic Distribution System 100. The digital content label provides the name of the Electronic Digital Content Store(s) 103 and any other information that may be required for the ClearingHouse(s) 105 to create a digital certificate for the Electronic Digital Content Store(s) 103. The digital certificate is sent to the digital content label in a secure fashion, and then forwarded by the digital content label to the Electronic Digital Content Store(s) 103. The ClearingHouse(s) 105 maintains a database of digital certificates that it has assigned. Each certificate includes a version number, a unique serial number, the signing algorithm, the name of the issuer (e.g., the name of ClearingHouse(s) 105), a range of dates for which the certificate is considered to be valid, the name Electronic Digital Content Store(s) 103, the public key of the Electronic Digital Content Store(s) 103, and a hash code of all of the other information signed using the private key of the ClearingHouse(s) 105. Entities that have the Public Key 621 of the ClearingHouse(s) 105 can validate the certificate and then be assured that a SC(s) with a signature that can be validated using the public key from the certificate is a valid SC(s).

[0173] After the Electronic Digital Content Store(s) 103 has received its digital certificate that was created by the ClearingHouse(s) 105 and the necessary tools for processing the SC(s) from the digital content label, it can begin offering Content 113 that can be purchased by End-User(s). The Electronic Digital Content Store(s) 103 includes its certificate and the Transaction SC(s) 640 and signs the SC(s) using its Digital Signature 643. The End-User Device (s) 109 verifies that the Electronic Digital Content Store(s) 103 is a valid distributor of Content 113 on the Secure Digital Content Electronic Distribution System 100 by first checking the digital certificate revocation list and then using the Public Key 621 of the ClearingHouse(s) 105 to verify the information in the digital certificate for the Electronic Digital Content Store(s) 103. A digital certificate revocation list is maintained by the ClearingHouse(s) 105. The revocation list may be included as one of the parts in a License SC(s) 660 that is created by the ClearingHouse(s) 105. End-User Device(s) 109 keep a copy of the revocation list on the End-User Device(s) 109 so they can use it as part of the Electronic Digital Content Store(s) 103 digital certificate validation. Whenever the End-User Device(s) 109 receives a License SC(s) 660 it determines whether a new revocation list is included and if so, the local revocation list on the End-User Device(s) 109 is updated.

B. Rights Management Processing

Order SC(s) Analysis

[0174] The ClearingHouse(s) 105 receives an Order SC(s) 650 from an End-User(s) after the End-User(s) has received the Transaction SC(s) 640, which include the Offer SC(s) 641, from the Electronic Digital Content Store(s) 103. The Order SC(s) 650 consists of parts that contain information relative to the Content 113 and its use, information about the Electronic Digital Content Store(s) 103 that is selling the Content 113, and information about the End-User (s) that is purchasing the Content 113. Before the ClearingHouse(s) 105 begins processing the information in the Order SC(s) 650, it first performs some processing to insure that the SC(s) is in fact valid and the data it contains has not been corrupted in any way.

Validation

[0175] The ClearingHouse(s) 105 begins the validation of Order SC(s) 650 by verifying the digital signatures, then the ClearingHouse(s) 105 verifies the integrity of the Order SC(s) 650 parts. To validate the digital signatures, first the ClearingHouse(s) 105 decrypts the Contents 631 of the signature itself using the Public Key 661 of the signing entity included if signed. (The signing entity could be the Content Provider(s) 101, the Electronic Digital Content Store(s) 103, the End User Device(s) 109 or any combination of them.) Then, the ClearingHouse(s) 105 calculates the digest of the concatenated part digests of the SC(s) and compares it with the digital signature's decrypted Content 113. If the two values match, the digital signature is valid. To verify the integrity of each part, the ClearingHouse(s) 105 computes the digest of the part and compares it to the digest value in the BOM. The ClearingHouse(s) 105 follows the same process to verify the digital signatures and part integrity for the Metadata and Offer SC(s) 641 parts included within the Order SC(s) 650.

[0176] The process of verification of the Transaction and Offer SC(s) 641 digital signatures also indirectly verifies that the Electronic Digital Content Store(s) 103 is authorised by the Secure Digital Content Electronic Distribution System 100. This is based on the fact that the ClearingHouse(s) 105 is the issuer of the certificates. Alternately, the ClearingHouse(s) 105 would be able to successfully verify the digital signatures of the Transaction SC(s) 640 and Offer SC(s) 641 using the public key from the Electronic Digital Content Store(s) 103, but only if the entity signing the SC(s) has ownership of the associated private key. Only the Electronic Digital Content Store(s) 103 has ownership of the

during Content 113 purchase transactions and report request transactions. The information can be used for a variety of purposes such as audits of the Secure Digital Content Electronic Distribution System 100, generation of reports, and data mining.

[0186] The ClearingHouse(s) 105 also maintains account balances in Billing Subsystem 182 for the Electronic Digital Content Store(s) 103. Pricing structures for the Electronic Digital Content Store(s) 103 is provided to the ClearingHouse (s) 105 by the digital content labels. This information can include things like current specials, volume discounts, and account deficit limits that need to be imposed on the Electronic Digital Content Store(s) 103. The ClearingHouse(s) 105 uses the pricing information to track the balances of the Electronic Digital Content Store(s) 103 and insure that they do not exceed their deficit limits set by the Content Provider(s) 101.

[0187] The following operations are typically logged by the ClearingHouse(s) 105:

- End-User Device(s) 109 requests for License SC(s) 660
- Credit card authorisation number when the ClearingHouse(s) 105 handles the billing
- Dispersement of License SC(s) 660 to End-User Device(s) 109
- Requests for reports
- Notification from the End-User(s) that the Content SC(s) 630 and License SC(s) 660 were received and validated

[0188] The following information is typically logged by the ClearingHouse(s) 105 for a License SC(s) 660:

- Date and time of the request
- Date and time of the purchase transaction
- Content ID of the item being purchased
- Identification of the Content Provider(s) 101
- Store Usage Conditions 519
- Watermarking instruction modifications
- Transaction ID 535 that was added by the Electronic Digital Content Store(s) 103
- Identification of the Electronic Digital Content Store(s) 103
- Identification of the End-User Device(s) 109
- End-User(s) credit card information (if the ClearingHouse(s) 105 is handling the billing)

[0189] The following information is typically logged by the ClearingHouse(s) 105 for an End-User's credit card validation:

- Date and time of the request
- Amount charged to the credit card
- Content ID of the item being purchased
- Transaction ID 535 that was added by the Electronic Digital Content Store(s) 103
- Identification of the Electronic Digital Content Store(s) 103
- Identification of the End-User(s)
- End-User(s) credit card information
- Authorisation number received from the clearer of the credit card

[0190] The following information is typically logged by the ClearingHouse(s) 105 when a License SC(s) 660 is sent to an End-User Device(s) 109:

- Date and time of the request
- Content ID of the item being purchased
- Identification of Content Provider(s) 101
- Usage Conditions 517
- Transaction ID 535 that was added by the Electronic Digital Content Store(s) 103
- Identification of the Electronic Digital Content Store(s) 103
- Identification of the End-User(s)

[0191] The following information is typically logged when a report request is made:

- Date and time of the request
- Date and time the report was sent out
- Type of report being requested

Electronic Digital Content Store(s) 103 includes a flag in the Transaction SC(s) 640 that is carried forward to the ClearingHouse(s) 105 in the Order SC(s) 650. The ClearingHouse(s) 105 interprets the flag in the Order SC(s) 650 and proceed with the transaction without charging the End-User(s) for the purchase of the Content 113.

VIII. CONTENT PROVIDER

A. Overview

[0200] The Content Provider(s) 101 in the Secure Digital Content Electronic Distribution System 100 is the digital content label or the entity who owns the rights to the Content 113. The role of the Content Provider(s) 101 is to prepare the Content 113 for distribution and make information about the Content 113 available to Electronic Digital Content Store(s) 103 or retailers of the downloadable electronic versions of the Content 113. To provide the utmost security and rights control to the Content Provider(s) 101, a series of tools are provided to enable the Content Provider(s) 101 to prepare and securely package their Content 113 into SC(s) at their premises so that the Content 113 is secure when it leaves the Content Provider(s)' 101 domain and never exposed or accessible by unauthorised parties. This allows Content 113 to be freely distributed throughout a non-secure network, such as the Internet, without fear of exposure to hackers or unauthorised parties.

[0201] The end goal of the tools for the Content Provider(s) 101 is to prepare and package a Content 113 such as a song or series of songs into Content SC(s) 630 and to package information describing the song, approved uses of the song (content Usage Conditions 517), and promotional information for the song into a Metadata SC(s) 620. To accomplish this, the following set of tools are provided:

- Work Flow Manager 154 - Schedules processing activities and manages the required synchronisation of processes.
- Content Processing Tools 155 - A collection of tools to control Content 113 file preparation including Watermarking, Preprocessing (for an audio example any required equalisation, dynamics adjustment, or re-sampling) encoding and compression.
- Metadata Assimilation and Entry Tool 161 - A collection of tools used to gather Content 113 description information from the Database 160 of the Content Provider(s) and/or third party database or data import files and/or via operator interaction and provides means for specifying content Usage Conditions 517. Also provided is an interface for capturing or extracting content such as digital audio content for CDS or DDP files.
- Quality Control Tool enables to preview of prepared content and metadata. Any corrections needed to the metadata or resubmission of the content for further processing can be conducted.
- SC(s) Packer Tool 152 - Encrypts and packages all Content 113 and information and calls the SC(s) Packer to pack into SC(s).
- Content Dispersement Tool (not shown) - Disperses SC(s) to designated distribution centres, such as Content Hosting Site(s) 111 and Electronic Digital Content Store(s) 103.
- Content Promotions Web Site 156 - stores Metadata SC(s) 620 and optionally additional promotional material for download by authorised Electronic Digital Content Store(s) 103.

B. Work Flow Manager 154

[0202] The purpose of this tool is to schedule, track, and manage Content 113 processing activities. This application enables multi-user access as well as allowing scheduling of Content 113 and status checking from remote locations within the Intranet or extranet of the Content Provider(s) 101. This design also allows for collaborative processing where multiple individuals can be working on multiple pieces of Content 113 in parallel and different individuals can be assigned specific responsibilities and these individuals can be spread throughout the world.

[0203] Turning now to FIG. 8 is a block diagram of the major processes of the Work Flow Manager 154 corresponding to FIG. 7. The major processes in FIG. 8 summarises the Content 113 processing functions provided by the tools described in this section. The Work Flow Manager 154 is responsible for feeding jobs to these processes and directing jobs to the next required process upon completion of its current process. This is accomplished through a series of Application Programming Interfaces (APIs) which each processing tool calls to:

- retrieve the next job to process
- indicate successful completion of a process
- indicate unsuccessful completion of a process and reason for the failure
- provide interim status of a process (to allow initiation of processes that require only partial completion of a dependent process)
- add comments to a product which are made available to the designated processes

the Content Provider(s) determines the Content selection process.

[0213] If the required information needed to perform a query to the Database 160 of the Content Provider(s) 101 is specified, the job is processed by the Automatic Metadata Acquisition Process 803. In a music embodiment, to properly schedule the product for audio processing, the product's genre and the desired compression levels are specified as well as the audio PCM or WAV filename(s). This information may be entered as part of the product selection process or selected via a customised query interface or Web browser function. Specification of this information enables the product to be scheduled for content processing.

[0214] The product selection user interface provides an option enabling the operator to specify whether the product can be released for processing or whether it are held pending further information entry. If held, the job is added to the queue of the New Content Request Process 802 awaiting further action to complete data entry and/or release the product for processing. Once the product is released, the Work Flow Manager 154 evaluates the information specified and determines which processes the job is ready to be passed to.

[0215] If adequate information is provided to enable an automated query to the Database 160 of the Content Provider (s)' 101, the job is queued for Automatic Metadata Acquisition Process 803. If the database mapping table has not been configured for the Automatic Metadata Acquisition Process 803, the job is queued for Manual Metadata Entry Process 804 (see Automatic Metadata Acquisition Process 803 section for details on the Database Mapping Table).

[0216] If the required general information for audio processing and the specific information required for watermarking is specified, the job is queued for Watermarking Process 808 (the first phase of content processing). If any of the required information is missing when the job is released, the job is queued to the queue of the Products Awaiting Action/ Information Process 801 along with status indicating the information that is missing.

[0217] If the status indicates that the filename of the Content 113, for example where the Content 113 is audio and the PCM or WAV file is missing, this may indicate that a capture (or digital extraction from digital media) is required. The audio processing functions require that the song files be accessible via a standard file system interface. If the songs are located on external media or a file system that is not directly accessible to the audio processing tools, the files are first be copied to an accessible file system. If the songs are in digital format but on CD or Digital Tape, they are extracted to a file system accessible to the audio processing tools. Once the files are accessible, the Work Flow Manager User Interface 700 is used to specify or select the path and filename for the job so that it can be released to the watermarking process, assuming all other information required for watermarking has also been specified.

3. Automatic Metadata Acquisition Process 803

[0218] The Automatic Metadata Acquisition Process 803 performs a series of queries to the Database 160 of the Content Provider(s) 101 or a staging database where data has been imported, in an attempt to obtain as much of the product information as possible in an automated fashion. The Automatic Metadata Acquisition Process 803 requires the following information prior to allowing items to be placed on its queue:

- database mapping table with adequate information to generate queries to the Database 160 of the Content Provider (s) 101
- product information required to perform queries
- adequate product information to uniquely define product

[0219] An automated query is performed to the Database 160 of the Content Provider(s) 101 to obtain the information necessary to process this Content 113. For example, if the Content 113 is music, the information needed to perform this query could be the album name or may be a UPC or a specific album or selection ID as defined by the Content Provider(s) 101. Of the information to be obtained, some is designated as required (see the section on Automatic Metadata Acquisition Process 803 for details). If all required information is obtained, the job is next queued for Usage Conditions Process 805. If any required information is missing, the song is queued for Manual Metadata Entry Process 804. If any jobs in the Products Awaiting Action/Information Process 801 queue are waiting for any of the information obtained in this step, the jobs status is updated to indicate that it is no longer waiting for this information. If that job no longer has any outstanding requirements, it is queued to the next defined queue.

4. Manual Metadata Entry Process 804

[0220] The Manual Metadata Entry Process 804 provides a means for an operator to enter missing information. It has no dependencies. Once all required information is specified, the job is queued for Usage Conditions Process 805.

- quality levels for product (could be preconfigured)
- compression algorithm (could be preconfigured)
- product genre (if required by preprocessor)

[0228] Upon completion of the encoding process, the jobs are queued to the Content Quality Control Process 810 if configured by the work flow rules. If not, the jobs are queued for Encryption Process 811.

[0229] If third party providers of encoding tools do not provide a method to display the percentage of the Content 113, such as audio, that has been processed or a method to indicate the amount of Content 113 that has been encoded as a percentage of the entire selection of Content 113 selected, in FIG. 11 there is shown a flow diagram 1100 of a method to determine the encoding rate of Digital Content for the Content Preprocessing and Compression tool of FIG. 8. The method begins with the selection of the desired encoding algorithm and a bit rate, step 1101. Next, a query is made to determine if this algorithm and encoding rate has a previously calculated rate factor, step 1102. The rate factor is the factor used to determine the rate of compression for a specific encoding algorithm and a specific bit rate. If no previously calculated rate factor is stored, a sample of the Content 113 is encoded for a predetermined amount of time. The predetermined period of time in the preferred embodiment is a few seconds. This rate of encoding for a predetermined period of time is used to calculate a new rate factor RNEW. Calculating a new rate factor RNEW knowing the amount of time and the amount of Content 113 encoded is RNEW = (length of Digital Content encoded)/(amount of time), step 1108. The Content 113 is encoded and the encoding status is displayed using the previously calculate rate factor RNEW, step 1109. This encoding rate factor RNEW is then stored, step 1107, for future use for this encoding algorithm and encoding bit rate. If the selected algorithm has a previously calculated rate factor RSTORED, step 1103. The Content 113 is encoded and the progression displayed using the previously calculated rate factor RSTORED, step 1104. In the meantime, a current rate factor, Rcurrent is calculated for this selected algorithm and bit rate, step 1105. This current rate factor Rcurrent is used to update the stored rate factor RNEW = AVERAGE OF (RSTORED + RCURRENT), step 1106. The iterative update of the rate factor enables the determination of the encoding rate to become more and more accurate with each subsequent use for a particular encoding algorithm and bit rate. The new rate RNEW is then stored for future use, step 1107. The updating of RSTORED may not be made if the current rate factor R current is out range for the previously stored rate factor RSTORED by a given range or threshold.

[0230] The display of the encoding status can then be presented. The encoding status includes along with the current encoding rate, the display of the percentage of the total Content 113 displayed as a progression bar based on the encoding rate and the total length of the file for the Content 113. The encoding status can also include the time remaining for the encoding. The time remaining for the encoding can be calculated by dividing the encoding rate calculated RCURRENT by the total length of the file for Content 113. The encoding status can be transferred to another program that may invoke the calling process. This can help supervisory programs to encoding or co-dependent programs on encoding be operated and be batched for processing more efficiently. It should be understood, in an alternative embodiment, that encoding can include the step of watermarking.

10. Content Quality Control Process 810

[0231] The Content Quality Control Process 810 is similar in function to the Supervised Release Process 806. It is an optional step allowing someone to validate the quality of the content processing performed thus far. This has no dependencies other than completion of the Watermarking Process 808 and the encoding portion of the Preprocessing and Compression Process 809. Upon completion of the Content Quality Control Process 810 the following options are available:

- the jobs can be released and queued for Encryption Process 811.
- comments can be attached and one or more of the jobs re-queued for Preprocessing and Compression Process 809.

[0232] The last option requires that the unencoded watermarked version of the song file remain available until after Content Quality Control Process 810.

11. Encryption Process 811

[0233] The Encryption Process 811 calls the appropriate Secure Digital Content Electronic Distribution Rights Management function to encrypt each of the watermarked/encoded song files. This process has no dependencies other than completion of all other audio processing. Upon completion of the Encryption Process 811 process, the job is queued for Content SC(s) Creation Process 812.

on its way to step Before (the Metadata SC(s) Creation Process 807)
[needs the encryption keys].
coming from step Before (the Metadata SC(s) Creation Process 807)
on its way to either step A3 (the Final Quality Assurance Process 813) or step A4 (the Content Dispersement Process 814)
[needs the Content SC(s) 630].
coming from step C1 (the Watermarking Process 808)
on its way to step C2 (the Preprocessing and Compression Process 809)
[needs the metadata for Preprocessing and Compression Process 809].
coming from step C4 (the Encryption Process 811)
on its way to step C5 (the Content SC(s) Creation Process 812)
[needs the metadata for Content SC(s) 630 Packing]. coming from step C5 (the Content SC(s) Creation Process 812)
on its way to either step A3 (the Final Quality Assurance Process 813) or step A4 (the Content Dispersement Process 814) [needs the Metadata SC(s) 620].

A3: After step A3 (the Final Quality Assurance Process 813),
place onto queue B2 (Manual Metadata Entry Process 804),
or place onto queue B3 (Supervised Release Process 806),
or place into queue as required by the quality assurance operator.

A4: After step A4 (Content Dispersement Process 814),
the Work Flow Manager Tool 154 is done for this product.

B1: After step B1 (the Automatic Metadata Acquisition Process 803),
if the metadata needed for step C1 (the Watermarking Process 808) is present, then place an entry representing this product onto queue C1.
(do the following logic also)
if either 1- any required metadata is missing, or 2- there are comments directed to the manual metadata providers, then also place the product onto queue B2 (Manual Metadata Entry Process 804),
else if supervised release was requested for this product, then place the product onto queue B3 (Supervised Release Process 806).
else if the product has all the information from the Content Processing Tools 155 for all of the requested quality levels, then place the product onto queue Before (the Metadata SC(s) Creation Process 807),
else flag the product as needs the encryption keys and place the product onto queue A2 (Products Awaiting Action/Information Process 801).

B2: During step B2 (Manual Metadata Entry Process 804),
if step C1 (the Watermarking Process 808) has not been done and the metadata needed for step C1 is present, then place an entry representing this product onto queue C1.
(do the following logic also)
if metadata needed for step C2 the Preprocessing and Compression Process 809)just been provided, then
(do the following logic also)
if all the metadata that can be gathered by the Metadata Assimilation and Entry Tool 161 is present, then if supervised release was requested for this product, then place the product onto queue B3 (Supervised Release Process 806)
else
if all the information from step C4 (the Encryption Process 811) of the Content Processing Tools 155 is present, then place this product onto queue Before (the Metadata SC(s) Creation Process 807)
else flag the product as needs the encryption keys and place this product onto queue A2 (Products Awaiting Action/Information Process 801).
else
if the metadata provider requested a forced supervised release, then place the product onto queue B3 (Supervised Release Process 806)
else do nothing (keep the product on queue B2 (Manual Metadata Entry Process 804)).

B3: During step B3 (Supervised Release Process 806),
if this operator is sending the product back to step B2 (Manual Metadata Entry Process 804), then place the product on queue B2.
else if this operator released the product, then
if all the information from step C4 (the Encryption Process 811) of the Content Processing Tools 155 is present, then place this product onto queue Before (the Metadata SC(s) Creation Process)

- Supervised Release Tool

[0241] These tools enable Content Provider(s) 101 to implement the processes described above for Work Flow Manager 154. Tools described here are a toolkit based on Java in the preferred embodiment but other programming languages such as C/C++, Assembler and equivalent can be used.

1. Automatic Metadata Acquisition Tool

[0242] The Automatic Metadata Acquisition Tool provides a user the ability to implement the Automatic Metadata Acquisition Process 803 described above. The Automatic Metadata Acquisition Tool is used to access the Database 160 of the Content Provider(s) 101 and to retrieve as much data as possible without operator assistance. Configuration methods are available to automate this process. The Content Provider(s) 101 can tailor the default metadata template to identify the types of data this Content Provider(s) 101 wants to provide to End-User(s) (e.g., composer, producer, sidemen, track length) and the types of promotional data the Content Provider(s) 101 provides to the Electronic Digital Content Store(s) 103 (e.g., for a music example, sample clips by this artist, a history of this artist, the list of albums on which this recording appears, genres associated with this artist). The default metadata template includes data fields which are required by the End-User Device(s) 109, data fields which can be optionally provided to the End-User Device (s) 109 and a sample set of data fields, targeted to the Electronic Digital Content Store(s) 103, that promote the artist, album, and/or single.

[0243] To extract the template data fields from the Database 160 of the Content Provider(s) 101 the Automatic Metadata Acquisition Tool uses a table that maps the type of data (e.g., composer, producer, a biography of the artist) to the location within the database where the data can be found. Each of the Content Provider(s) 101 help specify that mapping table for their environment.

[0244] The Automatic Metadata Acquisition Tool uses a metadata template of the Content Provider(s) 101 and mapping table to acquire whatever data is available from the Databases 160 of the Content Provider(s) 101. The status of each product is updated with the result of the Automatic Metadata Acquisition Process 803. A product which is missing any required data is queued for Manual Metadata Entry Process 804, otherwise it is available for packing into a Metadata SC(s) 620.

2. Manual Metadata Entry Tool

[0245] The Manual Metadata Entry Tool provides a user the ability to implement the Manual Metadata Entry Process 804 described above. The Manual Metadata Entry Tool allows any properly authorised operator to provide the missing data. If the operator determines that the missing data is unavailable, the operator can attach a comment to the product and request supervised release. The Content Provider(s) 101 may require, for quality assurance reasons, that the product undergo supervised release. Once all the required data is present, and if supervised release has not been requested, then the product is available for packing into a Metadata SC(s) 620.

3. Usage Conditions Tool

[0246] The Usage Conditions Tool provides a user the ability to implement the Usage Conditions Process 805 described above. The process of offering Content 113 for sale or rent (Limited use), using electronic delivery, involves a series of business decisions. The Content Provider(s) 101 decides at which compression level(s) the Content 113 is made available. Then for each compressed encoded version of the Content 113, one or more usage conditions are specified. Each usage condition defines the rights of the End-User(s), and any restrictions on the End-User(s), with regard to the use of the Content 113.

[0247] As part of Content Processing Tools 155, a set of usage conditions (End-User(s) rights and restrictions) is attached to the product.

A usage condition defines:

1. the compression encoded version of the Content 113 to which this usage condition applies.
2. the type of user covered by this usage condition (e.g., business, private consumer)
3. whether this usage condition allows for the purchase or the rental of the Content 113. For a rental transaction:

- the measurement unit which is used to limit the term of the rental (e.g., days, plays).
- the number of the above units after which the Content 113 will no longer play.

For a purchase transaction:

- the number of playable copies the End-User(s) is allowed to make.

```
product ID        [src:content provider;]
                                          [dest: everybody;]
      licensor label company                    [dest: EMS; end-user;]
      licensee label company                    [dest: EMS; end-user;]
      source (publisher) of this object
      (sublicensee label company)               [dest: everybody;]
      type of object (i.e., a single object or an array of objects)
      object ID                                       [dest: everybody;]
        International Standard Recording Code (ISRC)
        International Standard Music Number (ISMN)

usage conditions  (src: content provider; dest: EMS, end-user,
ClearingHouse(s) 105)
purchased usage conditions    (src: EMS; dest: end-user, ClearingHouse(s)
105)
```

```
            title of song
            principal artist(s)
        }
        a pointer to {
            the artwork (e.g., album cover);
            the format of the artwork (e.g., GIF, JPEG);
        }

        optional info:

        an array of additional information {
            composer
            publisher
            producer
            sidemen
            date of recording
            date of release
            lyrics
            track name (description) / track length
            list of albums on which this recording appears
            genre(s)
        }
metadata 2  (src: content provider; dest: EMS)
    an array of structures, each representing different quality levels of
the same sound recording
    {
        the sound recording;
        the quality level of the sound recording;
        the size (in bytes) of the (probably compressed) sound recording;
    }

metadata 3  (src: content provider; dest: EMS, end-user)
    optional info:

    promotional material:
        a pointer to artist promotion material {
            a URL to the artist's web site;
            background description(s) of the artist(s);
            artist-related interviews (along with format of the
            interview (e.g., text, audio, video));
            reviews (along with format of the reviews (e.g., text,
            audio, video));
            sample clips (and its format and compression level);
```

queue may be required if the tool does not report terminating status.

[0253] A generic version of the Content Processing Tools 155 is described, but customisation is possible. The Content Processing Tools 155 can be written in Java, C/C++ or any equivalent software. The Content Processing Tools 155 can be delivered by any computer readable means including diskettes, CDS or via a Web site.

1. Watermarking Tool

[0254] The Watermarking Tool provides a user the ability to implement the Watermarking Process 808 as described above. This tool applies copyright information of the Content 113 owner to the song file using audio Watermarking technology. The actual information to be written out is determined by the Content Provider(s) 101 and the specific watermarking technology selected. This information is available to the front end Watermarking Tool so that it can properly pass this information to the watermarking function. This imposes a synchronisation requirement on the Metadata Assimilation and Entry Tool 161 to assure that it has acquired this information prior to, for example, allowing the song's audio file to be processed. This song will not be available for audio processing until the watermarking information has been obtained.

[0255] The watermark is applied as the first step in audio processing since it is common to all encodings of the song created. As long as the watermark can survive the encoding technology, the watermarking process need only occur once per song.

[0256] Various watermarking technologies are known and commercially available. The front end Watermarking Tool though is capable of supporting a variety of industry Watermarking Tools.

2. Preprocessing and Compression Tool

[0257] The Preprocessing and Compression Tool provides a user the ability to implement the Preprocessing and Compression Process 809 as described above. Audio encoding involves two processes. Encoding is basically the application of a lossy compression algorithm against, for a music content example, a PCM audio stream. The encoder can usually be tuned to generate various playback bit stream rates based on the level of audio quality required. Higher quality results in larger file sizes and since the file sizes can become quite large for high quality Content 113, download times for high quality Content 113 can become lengthy and sometimes prohibitive on standard 28,800 bps modems.

[0258] The Content Provider(s) 101 may, therefore, choose to offer a variety of digital content qualities for download to appease both the impatient and low bandwidth customers who don t want to wait hours for a download and the audiophile or high bandwidth customers who either only buys high quality Content 113 or has a higher speed connection.

[0259] Compression algorithms vary in their techniques to generate lower bit rate reproductions of Content 113. The techniques vary both by algorithm (i.e. MPEG, AC3, ATRAC) and by levels of compression. To achieve higher levels of compression, typically the data is re-sampled at lower sampling rates prior to being delivered to the compression algorithm. To allow for more efficient compression with less loss of fidelity or to prevent drastic dropout of some frequency ranges, the digital content may sometimes require adjustments to equalisation levels of certain frequencies or adjustments to the dynamics of the recording. The content preprocessing requirements are directly related to the compression algorithm and the level of compression required. In some cases, the style of Content 113 (e.g. musical genre) can be successfully used as a base for determining preprocessing requirements since songs from the same genre typically have similar dynamics. With some compression tools, these preprocessing functions are part of the encoding process. With others, the desired preprocessing is performed prior to the compression.

[0260] Besides the downloadable audio file for sale, each song also has a Low Bit Rate (LBR) encoded clip to allow the song to be sampled via a LBR streaming protocol. This LBR encoding is also the responsibility of the Content Processing Tools 155. This clip is either provided by the Content Provider(s) 101 as a separate PCM file or as parameters of offset and length.

[0261] As with watermarking, it is hoped that the encoding tools can be loaded via a DLL or command line system call interface and passed all the required parameters for preprocessing and compression. The front end Encoding Tool may have a synchronisation requirement with the Metadata Assimilation and Entry Tool 161, for example if the content is music, and if it is determined that the song's genre is acquired from the Database 160 of the Content Provider(s) prior to performing any audio preprocessing. This depends on the encoding tools selected and how indeterminate the genre for the song is. If the Content Provider(s) 101 varies the choice of encoded quality levels per song, this information is also be provided prior to the encoding step and agrees with the metadata being generated by the Metadata Assimilation and Entry Tool 161.

[0262] A variety of high quality encoding algorithms and tools are known today. The front end Encoding Tool though is capable of supporting a variety of industry encoding tools.

[0263] Turning now to FIG. 12 is shown a flow diagram of one embodiment for the Automatic Metadata Acquisition Tool of FIG. 8 according to the present invention. The process starts with reading an identifier from the media the

as a metadata file to be included in the Metadata SC(s) 620.

F. Final Quality Assurance Tool

[0270] The Final Quality Assurance Tool provides a user the ability to implement the Final Quality Assurance Process 813 as described above. Once all the SC(s) have been built for a content file, the content is available for a final quality assurance check. Quality assurance can be performed at various stages of the Content 113 preparation process. The Content Provider(s) 101 can choose to perform quality assurance as each major step is completed to prevent excessive rework later or may choose to wait until all audio preparation processes are complete and perform quality assurance on everything at once. If the latter is chosen, quality assurance is performed at this point upon completion of the creation of the SC(s). This tool allows each SC(s) for the song to be opened, examined, and the audio played.

[0271] Any problem discovered, even minor text changes requires that the SC(s) be rebuilt due to internal security features of SC(s). To avoid unnecessary re-processing time, it is highly recommended that the interim quality assurance steps be utilised to assure accuracy of the metadata and that this specific quality assurance step be reserved for validating appropriate cross references between the SC(s) associated with this song. If problems are found, the assurer can enter a problem description to be attached to the song and have it re-queued to the appropriate processing queue for reprocessing. Status is updated appropriately in the Work Flow Manager 154 to indicate the status of all related components of the song. If no problems are discovered, the Content 113 is marked or flagged as ready for release.

G. Content Dispersement Tool

[0272] The Content Dispersement Tool provides a user the ability to implement the Content Dispersement Process 814 as described above. Once the Content 113 has been approved for release, the SC(s) for the Content 113 are placed in the queue of the Content Dispersement Process. The Content Dispersement Tool monitors the queue and performs immediate transfer of the SC(s) files or batch transfer of a group of SC(s) files based on the configuration settings provided by the Content Provider(s) 101. The Content Provider(s) 101 can also optionally configure the Content Dispersement Tool to automatically hold all SC(s) in this queue until they are manually flagged for release. This allows the Content Provider(s) 101 to prepare content in advance of their scheduled release date and hold them until they wish to release them e.g., a new song, movie or game. The SC(s) can also control access to Content 113 based on a defined release date so there is no requirement for the Content Provider(s) 101 to actually hold up delivery of the SC(s) but this manual release option can still be used for this purpose or used to manage network bandwidth required to transfer these large files.

[0273] When flagged for release, the Content SC(s) 630 for the Content 113 are transferred via FTP to the designated Content Hosting Site(s) 111. The Metadata SC(s) 620 is transferred via FTP to the Content Promotions Web Site 156. Here the SC(s) are staged to a new Content 113 directory until they can be processed and integrated into the Content Promotions Web Site 156.

[0274] FIG. 17 is a flow diagram of an alternate embodiment to automatically retrieve additional information for the Automatic Metadata Acquisition Tool of FIG. 8 according to the present invention. The process is similar for that described in FIG. 8 above. However, the quality checks of Supervised Release 806 and Content Quality Control 809 are combined into one quality check called Quality Control 1704. Performing quality checks prior to Metadata SC Creation 807 and Content SC Creation 812. Performing quality check prior to SC creation, eliminates the steps of unpacking the Content 113 and the associated Metadata SC(s) 620. In addition, in this embodiment, the queue of Products Awaiting Action/Information 801 have been eliminated. The jobs are placed on the specific process queues depending on what action is being requested. For example, if the job requires Manual Metadata, i.e. additional Metadata to be entered, the job is place on the Manual Metadata entry queue. Also the Automatic Metadata Acquisition 803 has been merged with New Content Request to occur up front prior to the Metadata Assimilation and Entry Tool 161 and the Content Processing Tool 155. Finally, it is important to point out that the Usage Conditions 804 are entered both at the Automatic Metadata Acquisition 803 and during the Manual Metadata Entry 803. Since, many of the usage conditions can be automatically filled-in during the Automatic Metadata Acquisition 803 step.

H. Content Promotions Web Site

[0275] To most effectively disperse information on what the Content Provider(s) 101 is making available for sale via digital download, and to get the necessary files to the Electronic Digital Content Store(s) 103 to enable it to make this Content 113 available for download to its customers, each Content Provider(s) 101 should have a secure web site housing this information. This is similar to the method used today by some Content Provider(s) 101 to make promotional content available to their retailers and others with a need for this information. In the case where this type of service already exists, an additional section can be added to the web site where Electronic Digital Content Store(s) 103 can

[0285] The End-User Device(s) 109 initiates the request for a Content SC(s) 630 by sending the License SC(s) 660 to the Content Hosting Site(s) 111. This is the same License SC(s) 660 returned by the ClearingHouse(s) 105. The Digital Signature of the License SC(s) 660 can be verified to determine if it is a valid License SC(s) 660. If it is a valid License SC(s) 660 either the download is initiated, or the download request may be redirected to another Content Hosting Site(s) 111.

2. Content Hosting Site(s) 111 provided by the Secure Digital Content Electronic Distribution System 100

[0286] For the Secure Digital Content Electronic Distribution System 100 the decision of which site should be used to download the Content 113 is made by the primary content site that received the initial request for a Content SC(s) 630. This site uses the following information to make this decision:

- Are there secondary content sites that host the Content 113 requested? (The majority of Content 113 offered by the Secure Digital Content Electronic Distribution System 100 is only located at primary sites);
- Where is the End-User Device(s) 109 geographically located? (This information can be obtained from the End-User Device(s) 109 when the request is initiated at the End-User Device(s) 109, this is passed up to the Clearing-House(s) 105 in the Order SC(s) 650;
- Is the appropriate secondary site up and operational? (Sometimes the secondary sites may be off-line);
- What is the load of the secondary sites? (In some cases where a secondary site is swamped with activity another site that is less busy may be selected.

[0287] Before transmitting the Content SC(s) 630 to the End-User Device(s) 109, analysis and verifications are performed on the End-User's request. A database is kept of all of the License SC IDs that have been used to download Content 113. This database can be checked to ensure that the End-User Device(s) 109 only makes one request for each piece of Content 113 purchased. This prevents malicious users from repeatedly accessing the Content Hosting Site(s) 111 in hopes of slowing down the Content Hosting Site(s) 111 and prevents unauthorised download of the Content SC(s) 630.

[0288] The promotion and demotion of Content 113 to the Secondary Content sites is done periodically based on customer demand for the individual pieces of Content 113.

Content Hosting Router

[0289] The Content Hosting Router (not shown) resides in the Content Hosting Site(s) 111 and receives all requests from End-User(s) wanting to download Content 113. It performs validation checks on the End-User(s) request to ensure they indeed bought the Content 113. A database is maintained on the status of the Secondary Content Sites that includes what Content 113 is on them and their current status. This current status includes the amount of activity on the sites and whether a site is down for maintenance.

[0290] The only interface to the Content Hosting Router is the License SC(s) 660 that is sent by the End-User Device (s) 109 when Content 113 is required to be downloaded. The License SC(s) 660 includes information that indicates the user is allowed to download the Content 113.

Secondary Content Sites

[0291] The Secondary Content Sites (not shown) host the popular Content 113 of the Secure Digital Content Distribution System 100. These sites are geographically dispersed across the world and are located near Network Access Points (NAPs) to improve download times. These sites are added to the system as demand on the primary Content Hosting Site(s) 111 nears maximum capacity

IX. ELECTRONIC DIGITAL CONTENT STORE(S)

A. Overview - Support for Multiple Electronic Digital Content Store(s) 103

[0292] Electronic Digital Content Store(s) 103 are essentially the retailers. They are the entities who market the Content 113 to be distributed to the customer. For distribution of Content 113, this would include Digital Content Retailing Web Sites, Digital Content Retail Stores, or any business who wishes to get involved in marketing electronic Content 113 to consumers. These businesses can market the sale of electronic Content 113 only or can choose to just add the sale of electronic goods to whatever other merchandise they currently offer for sale. Introduction of downloadable electronic goods into the service offering of the Electronic Digital Content Store(s) 103 is accomplished via a set of

create the files required to reference these downloadable objects as items in their own inventory. This process is batch driven and can be largely automated and is executed only to integrate new Content 113 into the site.

[0300] The tools for the Secure Digital Content Electronic Distribution have been designed to allow integration of sale of electronic downloadable Content 113 into typical implementations of web based Electronic Digital Content Store (s) 103 (i.e. Columbia House online, Music Boulevard, @Tower) and equivalent with minimal change to their current Content 113 retailing paradigm. Several methods of integration are possible and in the preferred embodiment, the Electronic Digital Content Store(s) 103 provides support for all product searches, previews, selections (shopping cart), and purchases. Each Electronic Digital Content Store(s) 103 establishes customer loyalty with its customers and continues to offer its own incentives and market its products as it does today. In the Secure Digital Content Electronic Distribution System 100, it would simply need to indicate which products in its inventory are also available for electronic download and allow its customers to select the electronic download option when making a purchase selection. In another embodiment, the customer's shopping cart could contain a mixture of electronic (Content 113) and physical media selections. After the customer checks out, and the Electronic Digital Content Store(s) 103 has completed the financial settlement and logged or notified its shipping and handling functions to process the physical merchandise purchased, the commerce handling function of the Electronic Digital Content Store(s) 103 then calls the Transaction Processor Module 175 to handle all electronic downloads. It simply passes the required information and all processing from that point on is handled by the toolset for the Secure Digital Content Electronic Distribution System 100. In another embodiment, other methods of transaction handling are also possible using tools for the Secure Digital Content Electronic Distribution System 100 to handle the financial settlement should the Electronic Digital Content Store(s) 103 wish to sell downloadable merchandise only or to segregate the financial settlement of physical and downloadable merchandise.

[0301] To handle the downloading of merchandise, the Electronic Digital Content Store(s) 103 is given a Product ID (not shown) for each downloadable product that it acquires from the Content Promotions Web Site 156 for the Content Provider(s) 101. This Product ID is associated to a customer's purchase selection to the downloadable product. The Product ID is what the Electronic Digital Content Store(s) 103 passes to the Transaction Processor Module 175 to identify the product that the user has purchased. The SC(s) (Offer SC(s) 641) that were created to describe the products, are isolated from the Electronic Digital Content Store(s) 103 and kept in an Offer Database 181 in an effort to simplify management of these objects and make their existence transparent to the Electronic Digital Content Store(s) 103.

[0302] The Transaction Processor Module 175 and other additional functions are provided as web server side executables (i.e. CGI and NSAPI, ISAPI callable functions) or simply APIs into a DLL or C object library. These functions handle run time processing for End-User(s) interactions and optional interactions with the ClearingHouse(s) 105. These functions interact with the web server's commerce services to create and download to the End-User Device(s) 109 the files necessary to initiate the Content 113 download process. They also handle optional interactions to provide authorisations and accept notifications of completion of activities.

[0303] An Accounting Reconciliation Tool 179 is also provided to assist the Electronic Digital Content Store(s) 103 in contacting the ClearingHouse(s) 105 to reconcile accounts based on its own and the transaction logs of the ClearingHouse(s) 105.

2. Content Acquisition Tool 171

[0304] The Content Acquisition Tool 171 is responsible for interfacing with the Content Promotions Web Site 156 to preview and download Metadata SC(s) 620. Since the Content Promotions site is a standard web site, a web browser is used by the Electronic Digital Content Store(s) 103 to navigate this site. The navigation features varies based on the site design of the Content Provider(s) 101. Some sites may provide extensive search capabilities with many screens of promotional information. Others may have a simple browser interface with lists of titles, performers or new releases to select from. All sites include the selection of Metadata SC(s) 620 containing all the promotional and descriptive information of a song or album.

[0305] Alternatively, the Electronic Store(s) 103 may subscribe to content updates and receive updates automatically via FTP.

Viewing Metadata

[0306] The Content Acquisition Tool 171 is a web browser helper application which launches whenever a Metadata SC(s) 620 link is selected at the Content Promotions Web Site 156. Selection of the SC(s) causes it to be downloaded to the Electronic Digital Content Store(s) 103, and launch the helper application. The Content Acquisition Tool 171 opens the Metadata SC(s) 620 and display the non-encrypted information contained therein. Displayed information includes Extracted Metadata 173, for a music example, the graphic image(s) associated with the song and the information describing the song, a preview clip of the song can also be listened to if included in the Metadata SC(s) 620.

[0313] Once the Offer SC(s) 641 is created, it is stored in an Offer Database 181 and is indexed with the Product ID pre-assigned in the Metadata SC(s) 620. This Product ID is used later by the Electronic Digital Content Store(s) 103 to identify the downloadable Content 113 being purchased by a customer when interfacing with the Offer Database 181 to retrieve the Offer SC(s) 641 for packaging and transmittal to the End-User(s). See the Transaction Processor Module 175 section for more details.

[0314] In another embodiment, the Electronic Digital Content Store(s) 103 hosts the Content SC(s) 641 at his site. This embodiment requires changes to the Offer SC(s) 641 such as the replacement of the URL of the Content Hosting Site(s) 111 with the URL of the Electronic Digital Content Store(s) 103.

3. Transaction Processing Module 175

[0315] Electronic Digital Content Store(s) 103 directs billing to ClearingHouse(s) 105. Alternatively, the Electronic Digital Content Store(s) 103 may request financial clearance direct from the ClearingHouse(s) 105. There are two basic modes for processing End-User(s) purchase requests for downloadable Content 113. If the Electronic Digital Content Store(s) 103 does not wish to handle the financial settlement of the purchase and has no special promotions or incentives governing the sale of the merchandise and does not use a shopping cart metaphor for batching the purchase requests, it may opt to provide links on its Content 113 download pages directly to the Offer SC(s) 641 files. These Offer SC(s) 641 would have to have been built with retail pricing information included in the metadata. Also included in the Offer SC(s) 641 is a special HTML offer page presenting the purchase options with terms and conditions of the sale. This page is built from a template created when the Offer SC(s) 641 was built. When the End-User(s) clicks on the direct link to the Offer SC(s) 641, the Offer SC(s) 641 is downloaded to the browser End-User Device(s) 109 launching a helper application which opens the container and present the offer page included in the Offer SC(s) 641. This page contains a form to collect customer information including credit card information and purchase option selection. The form then gets submitted directly to the ClearingHouse(s) 105 for financial settlement and processing. Optionally, this form may contain the fields needed to use the End-User(s)' credit information or industry standard local transaction handler.

[0316] An embodiment where the Electronic Digital Content Store(s) 103 handles billing is now described. The more typical mode of handling purchase requests is to allow the Electronic Digital Content Store(s) 103 to process the financial settlement and then submit the download authorisation to the End-User(s). This method allows the Electronic Digital Content Store(s) 103 to integrate sale of downloadable Content 113 with other merchandise offered for sale at his site, allows batch processing of purchase requests with only one consolidated charge to the customer (via a shopping cart metaphor) instead of individual charges for each download request, and allows the Electronic Digital Content Store(s) 103 to directly track his customers buying patterns and offer special promotions and club options. In this environment, the offer of downloadable Content 113 is included in his shopping pages which get added to a shopping cart when selected by the End-User(s) and get processed and financially settled as is done in the Electronic Digital Content Store(s)' 103 current shopping model. Once the financial settlement is completed, the commerce handling process of the Electronic Digital Content Store(s) 100 then calls the Transaction Processor Module 175 to complete the transaction.

Transaction Processor Module 175

[0317] The role of the Transaction Processor Module 175 is to put together the information needed by the End-User Device(s) 109 to initiate and process the download of the Content 113 purchased. This information is packaged into a Transaction SC(s) 640 which is sent back to the End-User Device(s) 109 by the Web Server as the response to the purchase submission. The Transaction Processor Module 175 requires three pieces of information from the commerce handling process of the Electronic Digital Content Store(s) 103: the Product IDs for the Content 113 purchased, Transaction Data 642, and an HTML page or CGI URL acknowledging the purchase settlement.

[0318] The Product ID is the value provided to the Electronic Digital Content Store(s) 103 in the Metadata SC(s) 620 associated to the Content 113 just sold. This Product ID is used to retrieve the associated Offer SC(s) 641 from the Offer Database 181.

[0319] The Transaction Data 642 is a structure of information provided by the transaction processing function of the Electronic Digital Content Store(s) 103 which is later used to correlate the ClearingHouse(s) 105 processing with the financial settlement transaction performed by the Electronic Digital Content Store(s) 103 and to provide user identity information to be included in the watermark of the Content 113 downloaded to the End-User Device(s) 109. When the ClearingHouse(s) 105 receives a valid Order SC(s) 650, it logs a transaction indicating the Content 113 that was sold, which Electronic Digital Content Store(s) 103 sold it and the associated Transaction Data 642 including the End-User's Name and a Transaction ID 535. The Transaction ID 535 provides a reference to the financial settlement transaction. This information is later returned by the ClearingHouse(s) 105 to the Electronic Digital Content Store(s) 103 for use in

flows 100 but are provided as options to allow the Electronic Digital Content Store(s) 103 the opportunity to close its records on the satisfaction of completion of the sale. It also provides information that may be needed to handle customer service requests by letting the Electronic Digital Content Store(s) 103 know what functions have transpired since financial settlement of the transaction or what errors occurred during an attempt to complete the sale. Alternatively, much of this status can be obtained from the ClearingHouse(s) 105 through the Customer Service Interface 184 as needed.

[0328] Frequency of notification of new Content 113 available at the Content Promotions Web Site 156 is determined by the Content Provider(s) 101. Notification may be provided as each new Metadata SC(s) 620 is added or just daily with all new Metadata SC(s) 620 added that day.

[0329] All of these notifications result in entries being made to the Transaction Log 178. If the Electronic Digital Content Store(s) 103 wishes to perform his own processing on these notifications, he can intercept the CGI call, perform his unique function and then optionally pass the request on to the Notification Interface Module 176.

5. Account Reconciliation Tool 179

[0330] This Account Reconciliation Tool 179 contacts the ClearingHouse(s) 105 to compare the Transaction Log 178 with the log of the ClearingHouse(s) 105. This is an optional process which is available to help the Electronic Digital Content Store(s) 103 feel comfortable with the accounting for the Secure Digital Content Electronic Distribution System 100.

[0331] In another embodiment, this tool can be updated to provide electronic funds transfers for automated periodic payments to the Content Provider(s) 101 and the ClearingHouse(s) 105. It can also be designed to automatically process payments upon reception of an electronic bill from the ClearingHouse(s) 105 after reconciling the bill against the Transaction Log 178.

C. Broadcast Electronic Digital Content Distribution Service

[0332] Broadcast primarily refers to a one to many transmission method where there is no personal interaction between the End-User Device(s) 109 and the Electronic Digital Content Store(s) 103 to customise on-demand viewing and listening. This is typically provided over a digital satellite or cable infrastructure where the Content 113 is preprogrammed so that all End-User Device(s) 109 receive the same stream.

[0333] A hybrid model can also be defined such that an Electronic Digital Content Store(s) 103 provides a digital content service organised in such a way that it can offer both a web distribution interface via an Internet connection as well as a higher bandwidth satellite or cable distribution interface via a broadcast service, with a great deal of commonality to the site design. If the IRD back -channel serial interface were connected to the web, and the IRD supported web navigation, the End-User(s) could navigate the digital content service in the usual way via the back-channel Internet interface, previewing and selecting Content 113 to purchase. The user can select high quality downloadable Content 113, purchase these selections, and receive the required License SC(s) 660 all via an Internet connection and then request delivery of the Content 113 (Content SC(s) 630) over the higher bandwidth broadcast interface. The Web service can indicate which Content 113 would be available for download in this manner based on the broadcast schedule or could build the broadcast streams based totally on purchased Content 113. This method would allow a Web based digital content service to contract with a broadcast facility to deliver high quality Content 113 to users equipped with the proper equipment making a limited number of specific Content 113 (e.g. songs or CDS) available daily in this manner and the entire catalog available for download in lower quality via the web interface.

[0334] Other broadcast models can be designed where there is no web interface to the End-User Device(s) 109. In this model, promotional content is packaged in specially formatted digital streams for broadcast delivery to the End-User Device(s) 109 (i.e. IRD) where special processing is performed to decode the streams and present the End-User (s) with the promotional content from which purchase selections can be made.

[0335] The actual purchase selections would still be initiated via back-channel communications from the End-User Device(s) 109 to the ClearingHouse(s) 105 and would utilise SC(s) to perform all data exchange. The toolset provided to the Electronic Digital Content Store(s) 103 has been architected and developed in such a way that most of the tools apply to both a point-to-point Internet service offering as well as a broadcast satellite or cable offering. The tools used by a Digital Content Web Site Electronic Digital Content Store(s) 103 to acquire and manage Content 113 as well as prepare SC(s) is also used by a satellite based Electronic Digital Content Store(s) 103 to manage and prepare Content 113 for distribution on a broadcast infrastructure. The SC(s) distributed over a Web service are the same as those distributed over a broadcast service.

offering sets. Users select and download video-clip static-offering packages 2006 by selecting an appropriate icon displayed while the video clip associated with each packages 2006 is played by the Set-Top Box(es) 1804. Users select and download video-catalog static offering by: (1) selecting an icon that displays the static offering catalog (i.e., an icon based graphical representation of the packages 2006 available in this set); (2) navigating the catalog to locate the desired selection; and (3) selecting the desired package. The Set-Top Box(es) 1804 communicates with the Broadcast Centre(s) 1802 to request the broadcast of this dynamic-offering package. The Broadcast Centre(s) 1802, collects all requests from the users Set-Top Box(es) 1804 and implements a scheduling algorithm that assigns packages 2006 to carousels and carousels to broadcast intervals. Once a dynamic offering package is assigned to a carousel (and therefore to a broadcast interval) it becomes a static-offering package.

[0342] All the packages 2006 promotional material, meta-data and descriptor are collected inside a master catalog. The master catalog is broadcasted in a pre-set carousel. The packages 2006 belonging to the static-offering set are listed in a bug catalog. The bug catalog contains the following:

- broadcast addressing and tuning information necessary to receive a package in the static offering set;
- broadcast addressing information for to receive the video clips;
- broadcast addressing information necessary to receive the master catalog;
- A pointer to the package associated with the video clip that is currently being broadcasted;
- A set of pointers representing the packages 2006 belonging to the static-offering set;
- The master catalog version; and
- The bug catalog version.

Since the bug catalog contains only pointers is very compact and it can be updated and downloaded frequently. In this fashion the Set-Top Box(es) 1804 can be continually up to date with the state of the broadcast channel

[0343] To build and represent the graphical user interface, the Set-Top Box(es) 1804 downloads the master catalog and extracts the contained data. To download a selected package the Set-Top Box(es) 1804 tunes to the carousels that contains the package and then starts collecting the data associated with the package. Package data is organised in sections. Due to digital transmission errors, sections maybe corrupted and/or lost. Sections integrity is determined using CRC-32 style information. In one embodiment, the Set-Top Box(es) 1804 gathers all the package sections over carousel cycles. After all sections have been collected and re-ordered the Set-Top Box(es) 1804 re-assembles the package. If a separate bi-directional unicast channel (such as the Internet) is available, the Set-Top Box(es) 1804 can use this channel to collect the missing package portion. Using the latter mechanism the package download time is reduced significantly.

[0344] A store manager application (not shown) in Broadcast Centre(s) 1802 is used to build the video-clip static-offering, video-catalog static-offering and the dynamic offering sets. The same application is used also to associate packages 2006 to carousels and determine the broadcast intervals of each carousel and each video clip. The actions performed by the broadcast manager application are implemented in real-time by the Broadcast Centre(s) 1802.

[0345] The package descriptors and the promotional material are broadcasted using a two-tier paradigm that allows for the real-time update of the receiver.

2. Web broadcasting Over Separate Channels Embodiment

[0346] FIG. 27 is a detailed block diagram of FIG. 18, illustrating an alternate embodiment of electronic distribution of digital content using separate channels in a web broadcasting service, according to the present invention. This exemplary architecture overview in FIG. 27 is used to illustrate a small number of changes that have to be made from the other embodiments for the delivery of music content over broadcast or telecommunications line. In particular, using current webcast infrastructure such as Hughs DirecPCTM only a few elements are added to adapt only embodiments of the present system to work with the existing Hughs DirecPCTM systems such as the trigger manager 2726 as described further below on End User Device(s) 109.

[0347] As described previously, the Broadcast Centre(s) 2702 receives the Offer SC(s) 641 from the Electronic Digital Content Store(s) 103. Along with the Offer SC(s) 641, the corresponding Content SC(s) 630 is retrieved. In this embodiment, the Offer SC(s) 641 and the Content SC(s) 630 are stored locally on computer storage device 2704. A web store 2706 running CGI or servlet scripts 2708 and 2710 takes the promotional content to form sample buttons and catalog listing as are depicted and further described in FIG. 28 below. To handle payment authorisations such as credit cards, debit cards and other payment verification systems, an eCommerce CGI 2710 interfaces with a financial clearing house 2710. The content placed on the Web Store 2706 is sent to a repository 2712.

[0348] In one embodiment, the content sent to the repository is in response to user selections received via a back channel from the End User Device(s) 109. Accordingly, in this embodiment, the content can be scheduled to match demand generated by the End User Device(s) 109. In addition, the periodicity of the content sent to the repository

by allowing user to make a certain number of purchases without reconnecting back to the ClearingHouse(s) 105 or the Web Store 2706. In this "off-line" embodiment, several categories may be used such as credit limits, purchase limits, periodic connection, limited time use of the Content 113 until reconnection is made within a certain period or vaoue deferment.

[0357] Once the cache manager 2720 completes the scheduling and downloading of the appropriate Content SC(s) 630 that have been requested, the trigger manager application 2726 notifies the Player Application 195 and the content is now available for importation from the Album_DSC(s) Buffer 2724 to the Player Application 196. In addition to notifying the Player Application that the Content SC(s) has been downloaded, other status can be reported back up to the Player Application 195 from the cache manager 2720 such as the status of the download, errors in the download and other information useful to a user in wishing to render or play the Content 113 desired.

[0358] And as previously described for the "online" or "connected" version of the current delivery system, the necessary steps of updating usage conditions and rights associated with the Content can be monitored through the Clearing House(s) 105.

X. END-USER DEVICE(S) 109

[0359] The applications in the End-User Device(s) 109 for the Secure Digital Content Electronic Distribution System 100 perform two main functions: first the SC(s) processing and copy control; and second playback of encrypted Content 113. Whether the End-User Device(s) 109 is a Personal Computer or a specialised electronic consumer device, it has to be capable of performing these base functions. The End-User Device(s) 109 also provides a variety of additional features and functions like creating play lists, managing the digital content library, displaying information and images during content playback, and recording to external media devices. These functions vary based on the services these applications are supporting and the type of devices the applications are designed for.

A. Overview

[0360] Referring now to FIG.10, shown is the major components and processes and End-User Device(s) 109 Functional Flow. The applications designed to support a PC based web interface Content 113 service consists of two executable software applications: the SC(s) Processor 192 and the Player Application 195. The SC(s) Processor 192 is an executable application which is configured as a Helper Application into the End-User(s) Web Browser 191 to handle SC(s) File/MIME Types. This application is launched by the Browser whenever SC(s) are received from the Electronic Digital Content Store(s) 103, the ClearingHouse(s) 105, and the Content Hosting Site(s) 111. It is responsible for performing all required processing of the SC(s) and eventually adding Content 113 to the Digital Content Library 196 of the End-User(s).

[0361] The Player Application 195 is a stand alone executable application which the End-User(s) loads to perform Content 113 in his Digital Content Library 196, manage his Digital Content Library 196 and create copies of the Content 113 if permitted. Both the Player Application 195 and SC(s) Processor 192 applications can be written in Java, C/C++ or any equivalent software. In the preferred embodiment, the applications can be downloaded from computer readable means such as website. However, other delivery mechanisms are also possible such as being delivered on computer readable media such as diskettes or CDS.

[0362] The searching and browsing of Content 113 information, previewing of, for example, song clips, and selecting songs for purchase is all handled via the End-User(s) Web Browser 191. Electronic Digital Content Store(s) 103 provides the shopping experience in the same way that is offered today by many Content 113 retailing web sites. The difference to the End-User(s) over today's web based Content 113 shopping is that they may now select downloadable Content 113 objects to be added to their shopping cart. If the Electronic Digital Content Store(s) 103 has other merchandise available for sale in addition to the downloadable objects, the End-User(s) may have a combination of physical and electronic downloadable merchandise in his shopping cart. The Secure Digital Content Electronic Distribution End-User Device(s) 109 are not involved until after the End-User(s) checks out and submits his final purchase authorisation to the Electronic Digital Content Store(s) 103. Prior to this point, all interaction is between the Web Server for the Electronic Digital Content Store(s) 103 and the Browser 191 on the End-User Device(s) 109. This includes preview of sample Digital Content clips. Digital Content clips are not packaged into SC(s) but instead are integrated into the web service of the Electronic Digital Content Store(s) 103 as downloadable files or fed from a streaming server. The format of the Content 113 clip is not dictated by the system architecture. In another embodiment, the Player Application 195 could interact directly with the Electronic Digital Content Store(s) 103 or ClearingHouse(s) 105 or offline using a promotional CD.

the download when the computer is next powered up.

[0371] When the scheduled download time occurs or if immediate download was requested, the SC(s) Processor 192 creates Order SC(s) 650 from information in the Transaction SC(s) 640, Offer SC(s) 641, and the Public Key 661 of the End-User(s) generated at install time. This Order SC(s) 650 is sent via HTTP request to the ClearingHouse(s) 105. When the ClearingHouse(s) 105 returns the License SC(s) 660, the Helper Application 198 is re-invoked to process the License SC(s) 660. The License SC(s) 660 is then opened and the URL of the Content Hosting Site(s) 111 is extracted from the referenced Order SC(s) 650. The License SC(s) 660 is then sent to the specified Content Hosting Site 111, via http request through the Browser, requesting download of the Content SC(s) 630. When the Content SC (s) 630 comes back to the Browser, the Helper Application 198 is re-invoked again. The SC(s) Processor 192 displays the name of the Content 113 being downloaded along with a download progress indicator and an estimated time to completion.

[0372] As the Content 113 is being received by the SC(s) Processor 192, it loads the Content 113 data into memory buffers for decryption. The size of the buffers depends on the requirements of the encryption algorithm and Watermarking technology 193 and is the minimum size possible to reduce the amount of unencrypted Content 113 exposed to hacker code. As a buffer is filled, it is decrypted using the Key 623 (corresponding to the Public Key 661) of the End-User(s) extracted from the License SC(s) 660, which itself is first decrypted using the Private Key. The decrypted buffer is then passed to the Watermarking function.

[0373] The Watermarking 193 extracts the Watermarking instructions from the License SC(s) 660 and decrypt the instructions using the Private Key of the End-User(s). The Watermarking data is then extracted from the License SC (s) 660 which includes transaction information such as the purchaser's name as registered with the Electronic Digital Content Store(s) 103 from which this Content 113 was purchased or derived from the credit card registration information if the Electronic Digital Content Store(s) 103 does not provide a registration function. Also included in the watermark is the purchase date and the Transaction ID 535 assigned by the Electronic Digital Content Store(s) 103 to reference the specific records logged for this transaction. The Store Usage Conditions 519 are also included to be used by the Copy Control of the Player Application 195.

[0374] The Watermarking 193 is protected with Tamper Resistant Code technology so as not to divulge the Watermarking instructions thus preventing a hacker from discovering the location and technique of the watermark. This prevents removal or modification of the watermark by a hacker.

[0375] After inscribing any required watermark to this content buffer, the buffer is passed to the scrambling function for Re-Encryption 194. A processor efficient secure encryption algorithm such as IBM's SEAL encryption technology is used to re-encrypt the Content 113 using a random Symmetric Key. Once the download and Decryption and Re-Encryption 194 process is complete, the encryption Key 623 used by the Content Provider(s) 101 to originally encrypt the Content 113 is now destroyed and the new SEAL key is itself encrypted using the Secret User Key created and hidden at installation time. This new encrypted Seal Key is now stored in the License Database 107.

[0376] Unlike source performed at the Content Provider(s) 101 and user Watermarking performed at the End User Device(s) 109 may need to become an industry standard to be effective. These standards are still evolving. The technology is available to allow control information to be embedded in the music and updated a number of times. Until such time as the copy control standards are more stable, alternative methods of copy control have been provided in the Secure Digital Content Electronic Distribution System 100 so that it does not rely on the copy control watermark in order to provide rights management in the consumer device. Storage and p lay/record usage conditions security is implemented utilising encrypted DC Library Collections 196 that are tied to the End User Device(s) 109 and protected via the Tamper Resistant Environment. Software hooks are in place to support copy control Watermarking when standards have been adopted. Support exists today for Watermarking AAC and other encoded audio streams at a variety of compression levels but this technology is still somewhat immature at this time to be put to use as a sole method of copy control.

[0377] The Decryption and Re-Encryption 194 process is another area of the code that is protected with Tamper Resistant Code technology so as not to divulge the original Content 113 encryption key, the new SEAL key, the Secret User Key, and where the Secret User Key segments are stored and how the key is segmented.

[0378] The process of Decryption and Re-Encryption 194 serves two purposes. Storing the Content 113 encrypted with an algorithm like SEAL enables faster than real-time decryption and requires much less processor utilisation to perform the decryption than does a more industry standard type algorithm like DES. This enables the Player Application 195 to perform a real-time concurrent decryption-decode-playback of the Content 113 without the need to first decrypt the entire file for the Content 113 prior to decode and playback. The efficiency of the SEAL algorithm and a highly efficient decode algorithm, allows not only concurrent operation (streaming playback from the encrypted file) but also allows this process to occur on a much lower powered system processor. Thus this application can be supported on a End-User Device(s) 109 as low end as a 60MHz Pentium system and perhaps lower. Separating the encryption format in which the Content 113 is finally stored from the original encryption format, allows for greater flexibility in the selection of the original content encryption algorithm. Thus use of widely accepted and proven industry standard al-

that the design establishes no definitive layout of these components. One such layout is provided in the generic player. Based on requirements from Content Provider(s) 101 and/or Electronic Digital Content Store(s) and other requirements, alternate layouts are possible.

[0388] This set is grouped into subgroups, starting with the components used to present End-User Display 1510 and handle controls called End-User Controls 1511 used for such low-level functions as audio playback , and presentation of metadata. Next, the End-User Display Component 1510 is further divided by special function groupings (Play-list, Digital Content Library), and then object-container components used for grouping and placing of those lower-level components.

[0389] Within the component listings below, any reference to creating CDS or copying of Content 113 to a CD or other recordable medium only applies to the case where the Player Application 195 has such functionality enabled. Also note that the term CD in that context is a generic one, that can also represent various other external recording devices, such as MiniDisc or DVD.

[0390] FIG. 16 is an example user interface screens of the Player Application 195 of FIG. 15 according to the present invention. Function for the End-User Controls 1511 include (corresponding screens of an End-User Interface are shown 1601-1605):

[0391] Controls for performing the Content 113:

- Play/Stop button
- Play button
- Stop button
- Pause button
- Skip forward button
- Skip backward button
- Volume control
- Track position control/display
- Audio channel volume level display and more.

[0392] Controls for the displaying metadata associated with the Content 113

- Cover Picture button
- Cover Picture object
- Artist Picture button
- Artist Picture object
- Track List button
- Track List Information object
- Track List Selector object (click to play)
- Track Name object
- Track Information object
- Track Lyrics button
- Track Lyrics object
- Track Artist Name object
- Track Credits button
- Track Credits object
- CD Name object
- CD Credits button
- CD Credits object
- Generic (Configurable) Metadata button
- Generic Metadata object and more.

[0393] Function for the End-User Display 1510 include (corresponding screens of an End-User Interface are shown 1601 - 1605):

[0394] Play-list of display container

- Play-list Management button
- Play-list Management window
- Digital Content search button
- Digital Content search Definition object
- Digital Content search Submit button

duplicating or copying the Content 113 stored at the End User Device(s) 109, on to an external device such as DVD Disc, digital tape, flash memory, mini Disc or equivalent read/writeable removable media, the use is updates to the logging site. This may be a precondition to copying the Content 113 in the usage conditions 206 that is transmitted when the Content 113 is purchased. This ensures the Content Provider(s) 101 can accurately track the usage of their Content 113 during their playing, duplicating or other actions upon the Content 113.

[0399] In addition, other information about the Content 113 can be uploaded to the logging site. For example the last time (e.g., hour and day) the Content 113 was performed; how many times the Content 113 was performed; if the Content 113 has been duplicated or copied to an authorised external device such as DVD Disc, digital tape or mini-Disc. In cases where there are multiple distinct users of a single Player Application 195 on the End User Device(s) 109, such as different members of a family, the identifications of the user of the Content 113 is transmitted along with the usage information to the logging site. By reviewing the usage information uploaded to the logging site, the Content Provider(s) 101 can measure the popularity of the Content 113 base on the actual usage, the identification of the user and the number of times the Content 113 has been performed. The actual usage measurement makes this system more factual driven over systems using sampling methods, such as a Nielsen Rating scheme for televisions, or telephone surveys, where only a limited number of users are sampled at any one time and the results extrapolated. In this present embodiment, the actual usage can be measures for the users logging back onto a designated web site such as the Electronic Digital Content Store(s) 103 or Content Provider(s) 101.

4. Decryption 1505, Decompression 1506 and Playback Components 1506

[0400] These components use the keys acquired by the Copy/Play Management components to unlock the audio data acquired from the Data Management and Library Access components, apply the appropriate decompression to prepare it for playback, and use system audio services to play it. In an alternate embodiment, the audio data acquired from the Data Management and Library Access components may be copied to removable media such as CDS, diskettes, tapes or MiniDisks.

5. Data Management 1502 and Library Access Components 1503

[0401] These components are used to store and retrieve song data on various storage devices on the End-User(s) ' system, as well as handle requests for information about the stored songs.

6. Inter-application Communication Components 1508

[0402] These components are used for coordination between the Secure Digital Content Electronic Distribution Player and other applications (e.g., Browser, helper-app and/or plug-in, etc) that may invoke the Player Application 195, or that the Player Application 195 needs to use when carrying out its functions. For example, when a URL control is activated, it invokes the appropriate browser and instruct it to load the appropriate page.

7. Other Miscellaneous Components

[0403] Individual components that don t fall into the categories above (e.g., Installation) are grouped here.

8. The Generic Player

[0404] In this section the combining of the components above into a version of the Player Application 195 is discussed. This is just one of many different examples possible, since the Player Application 195 is designed for customisation by being based on software objects. The Player Object Manager 1501 is a software framework holding all the other components together. As discussed in the sections above, the blocks below the Player Object Manager 1501 in this diagram are required for any player, but may be replaced by specialised versions depending on such things as form of encryption or scrambling being used, types of audio compression, access methods for the Content 113 library, and more.

[0405] Above the Player Object Manager 1501 are Variable Objects 1512, which are mostly derived from the metadata associated with the Content 113 being played or searched. These Variable Objects are made available to the End-User Device(s) 109 by way of the End-User Display 1510 and received input from the End-User Controls 1511. All objects are configurable, and the layouts of all containers are customisable. These objects may be implemented in C/C++, Java or any equivalent programming language.

within the Play-list, and does not alter information about the song stored within the Digital Content Library 196. These things can be changed:

* Displayed Song Title
* End-User(s) notes about the song
* Lead-in delay on playing the song
* Follow-on delay after playing the song
* Start-point within song when playing
* End-point within song when playing
* Weighting for random mode
* Volume adjustment for this song and more. Set Play-list attributes: Display and allow changes to the attributes of this Play-list. These attributes may be set:
* Play-list title
* Play-list mode (random, sequential, etc)
* Repeat mode (play once, restart when done, etc)
* End-User(s) notes about this Play-list Librarian (corresponding screen of an End-User Interface 1601):
* Open the Digital Content Librarian window. Also see Digital Content Librarian below for more info.

Song Play

[0411] When a song has been prepared for play, either by invoking the Player Application 195 with the song as an argument or by selecting a song for play from a Play-list or within the Digital Content Librarian, these are the End-User (s)' options: (corresponding screen of an End-User Interface 1601):

* Play
* Pause
* Stop
* Skip Backward
* Skip Forward
* Adjust Volume
* Adjust Track Position
* View Lyrics
* View Credits
* View CD Cover
* View Artist Picture
* View Track Information
* View other metadata
* Visit web site
* Play-list
* Librarian and more.

Digital Content Librarian

[0412] The Digital Content Librarian can be invoked implicitly when selecting songs or Play-lists (see above) or may be opened in its own window for management of the Song Library on the End-User(s)' system. In that case, these are the End-User(s)' options:

Working with songs:

Sort by Name
Sort by Category
Search by Keyword
Search by Included Song Title
Load Selected Play-list
Rename Play-list
Delete Play-list
Create CD from Selected Play-list (if enabled) and more.

Work with Play-lists:

191 and associated parts including Secure Container Processor 191, Helper Application 193, Water Marking 193 and Decryption Re-encryption 194 are not changed. This provides developers one set of APIs and Tools to build players for both this broadcast embodiment and the telecommunication embodiment or the computer readable medium embodiment. In addition, a Clearinghouse Emulator 1914, allows the transaction to be logged until the user connects the End User Device(s) 109 back to ClearingHouse(s) 105 for final account reconciliation.

[0419] Turning now to FIG. 21, shown is a flow diagram 2100 for a process running on the End User Device for purchasing content over the alternate embodiment of FIG. 18, according to the present invention. To better understand this flow diagram, reference will be made to FIGS. 22- 27 which are a series of screen shots illustrating the user's purchase on a television 1806 using the alternate embodiment of FIG. 18, according to the present invention.

[0420] The process flow 2100 begins in step 2102, a "Buy" and "Catalog" icons are displayed. User input, step 2104 is received. A test is made to determine the user selection, steps 2106 and 2108, of "Buy or Catalog" during the broadcast of a program 2204. If "Buy" is selected, the user is asked to identify themselves for billing purposes, step 2110. The embodiment shown in steps 2110-2116 and FIG. 24. uses a "smart card" and an associated personal identification number (PIN). Other billing mechanisms are possible, including the use of a debit card. Once the user identifies himself or herself, the download begins, step 2118. If "Catalog" is selected in step 2106, a menu panel of purchasable products is displayed, step 2120, and the user may navigate among them via a selection cursor (steps not shown). User input is received in step 2122. If this input it "Buy" the viewer proceeds through the authentication process, 2110-2116. If the input is "Exit", the viewer returns to the "Buy" and "Catalog" choices, step 2126. Upon successful authentication, the download process begins with an optional message indicating this to the viewer, as shown in FIG. 26. Note that all graphic images are overlaid on top of video that is not interrupted by the consumer's)?) purchasing activity.

[0421] It should be understood to those skilled in the art, that the broadcast embodiment of the present invention, allows for:

- Fast and reliable download of digital content over digital television broadcast infrastructure (where the digital content is a package, to be downloaded as a unit for later play; "play" being used broadly to refer to any form of ingest and interpretation);
- Self-contained description of the digital content over the digital television broadcast infrastructure. This system allows for the download of digital content over digital television broadcast infrastructure when a return channel from the content receiver to the content sender is not available (or infrequently available);
- Improved download time when a return channel from the content receiver to the content sender is available;
- Users to select and download digital content using a digital Set-Top Box(es) 1804 and a TV connected to the digital television broadcast infrastructure;
- Users to select and download digital content while simultaneously watching a video program;
- Content Providers to promote the digital content, available for download, using graphics and video;
- Managers to update, in real-time, the number and type of digital content available for download;

2. Web broadcasting Over Separate Channels Embodiment

[0422] An alternate embodiment of the End User Device(s) 109 using separate channels in a web broadcasting service, according to the present invention broadcast delivery is now described. Returning to FIG. 27, shown is an alternate embodiment for receiving Content 113 using separate channels in a web broadcasting infrastructure. FIG. 28 is a flow diagram 2800 for a process running on the End User Device for purchasing content over the alternate embodiment of FIG. 27, according to the present invention. The Set-Top Box(es) 1804 receives web pages composed by the Web Store 2306 such as the exemplary illustrations of the user screens shown in FIGS. 29-38 below.

[0423] The following is a description using the flow diagram 2800 of FIG. 28 with reference to the exemplary user screens of FIGs. 29-38. The process begins in step 2802 with promotional material being downloaded over a web cast channel to a promo cache 2322. In the event the user selects the button labelled "Album List"a selection list as show in FIG. 29 is presented, step 2806. In this example three selections are possible "Madonna", "Fleetwood Mac", and "Jewel". More or less selections can be shown and this just illustrates a one example. If the user makes a selection such as "Madonna" more information is presented about the artist in FIG. 30, step 2810. Note the possibility of previewing samples of the music with the "Sample" buttons. When a user selects the "Sample" button a promotional clip is played through the Web browser 191 or alternately through Player Application 191. If the user selects to purchase a selection a screen is presented to verify the "Account" and "Password" in FIG. 31, steps 2812 and 2814. In this example, the account information can be synchronised back with the Web Store 2306 or synchronised latter with the ClearingHouse(s) 105 as decided by the provider of the Content 113. The cache manager 2320 examines the Album + DSC(s) Buffer 2324 to determine if the corresponding Content SC(s) 630 is locally available for retrieval. If the correct Content SC(s) is available, it is retrieved and passed to the Player Application 195 for processing selects. In the event

channels, the method comprising the steps of:

receiving promotional metadata from a first web broadcast channel, the promotional metadata related to data available for reception;
assembling at least part of the promotional metadata into a promotional offering for review by a user;
selecting by a user, data to be received related to the promotional metadata;
receiving data from a second web broadcast channel, the data selected from the promotional metadata, and wherein the data has been previously encrypted using a first encrypting key; and
receiving the first decrypting key via a computer readable medium, the first decrypting key for decrypting at least some of the data received via the second web broadcast channel.

8. A method as claimed in claim 7, wherein the step of assembling at least part of the promotional data includes assembling at least part of the promotional data into a format readable by a web browser and wherein the step of selecting includes selecting with a web browser.

9. A method as claimed in claim 7, wherein the step of selecting includes selecting promotional material that have been previously received and stored on the user's system.

10. A method as claimed in claim 9, wherein the step of selecting further comprises the sub-steps of:

determining the schedule for the next web broadcast of the data selected; and
setting a trigger to trigger the user's system to receive the next web broadcast on the second channel.

11. A method as claimed in claim 10, wherein the step of receiving data from a second web broadcast channel, includes receiving the data selected from the promotional metadata on a web broadcast channel and a time provided by the trigger.

12. A method as claimed in claim 7, wherein the step of receiving data from a second web broadcast channel includes receiving data in a format compatible with the DirecPC™ system.

13. A method as claimed claim 7, wherein the step of receiving data from a second web broadcast channel include the sub-step of:
authorising over a back channel that the user's system is authorised to receive the data selected; and wherein the step of receiving the first decrypting key includes receiving the first decrypting key only if the user's system is authorised to receive the data selected.

14. A method as claimed in claim 7, wherein the step of receiving data from a second web broadcast channel further includes the sub-step of:
notifying the user the next time the user starts the user's system a status if the data selected from the promotional metadata has been received on the user's system.

15. A method as claimed in claim 7, wherein the step of receiving the first decrypting key, includes receiving the first decrypting key that has been encrypted with a second encrypting key.

16. A method as claimed in claim 15, wherein the step of receiving the first decrypting key includes receiving the first decrypting key over a broadcast stream.

17. A method as claimed in claim 15, wherein the second decrypting key is sent to the user's system from a clearinghouse.

18. A method as claimed in claim 15, wherein the second decrypting key has a timeout provision for decrypting data that has been encrypted with the second encryption key is sent to the user's system from a clearinghouse.

19. A system for securely providing data to a user's system over a web broadcast infrastructure with a plurality of channels, the system comprising:

a content system;
a first public key;

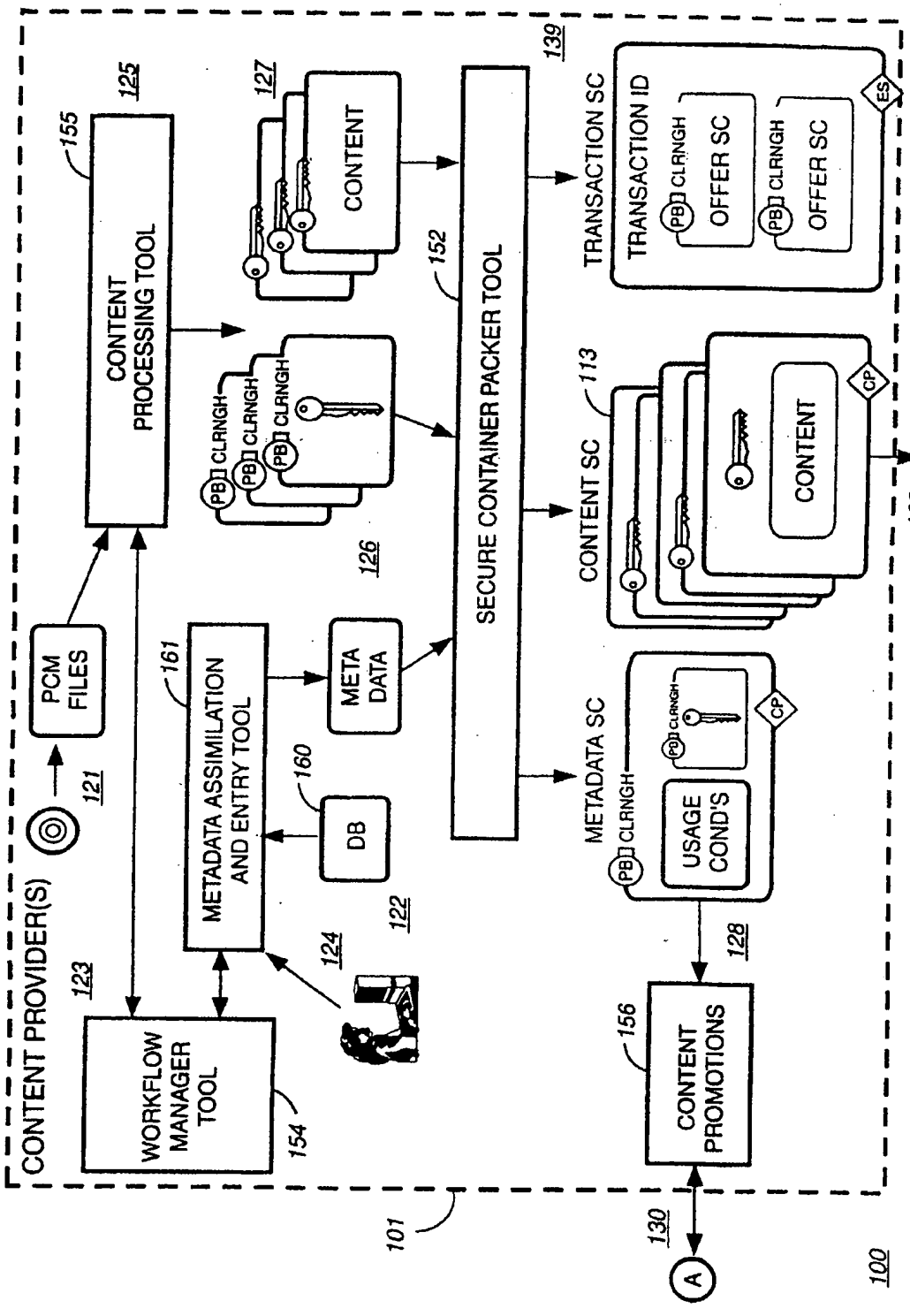

CONTENT PROVIDER(S)
121
123
PCM FILES
155
CONTENT PROCESSING TOOL
125
WORKFLOW MANAGER TOOL
154
METADATA ASSIMILATION AND ENTRY TOOL
161
160
DB
122
124
META DATA
126
PB CLRNGH
PB CLRNGH
PB CLRNGH
127
CONTENT
152
SECURE CONTAINER PACKER TOOL
139
TRANSACTION SC
TRANSACTION ID
PB CLRNGH
OFFER SC
PB CLRNGH
OFFER SC
ES
CONTENT SC
113
CONTENT
GP
129
B
METADATA SC
PB CLRNGH
USAGE COND'S
PB CLRNGH
CP
128
156
CONTENT PROMOTIONS
130
A
101
100

FIG. 1A

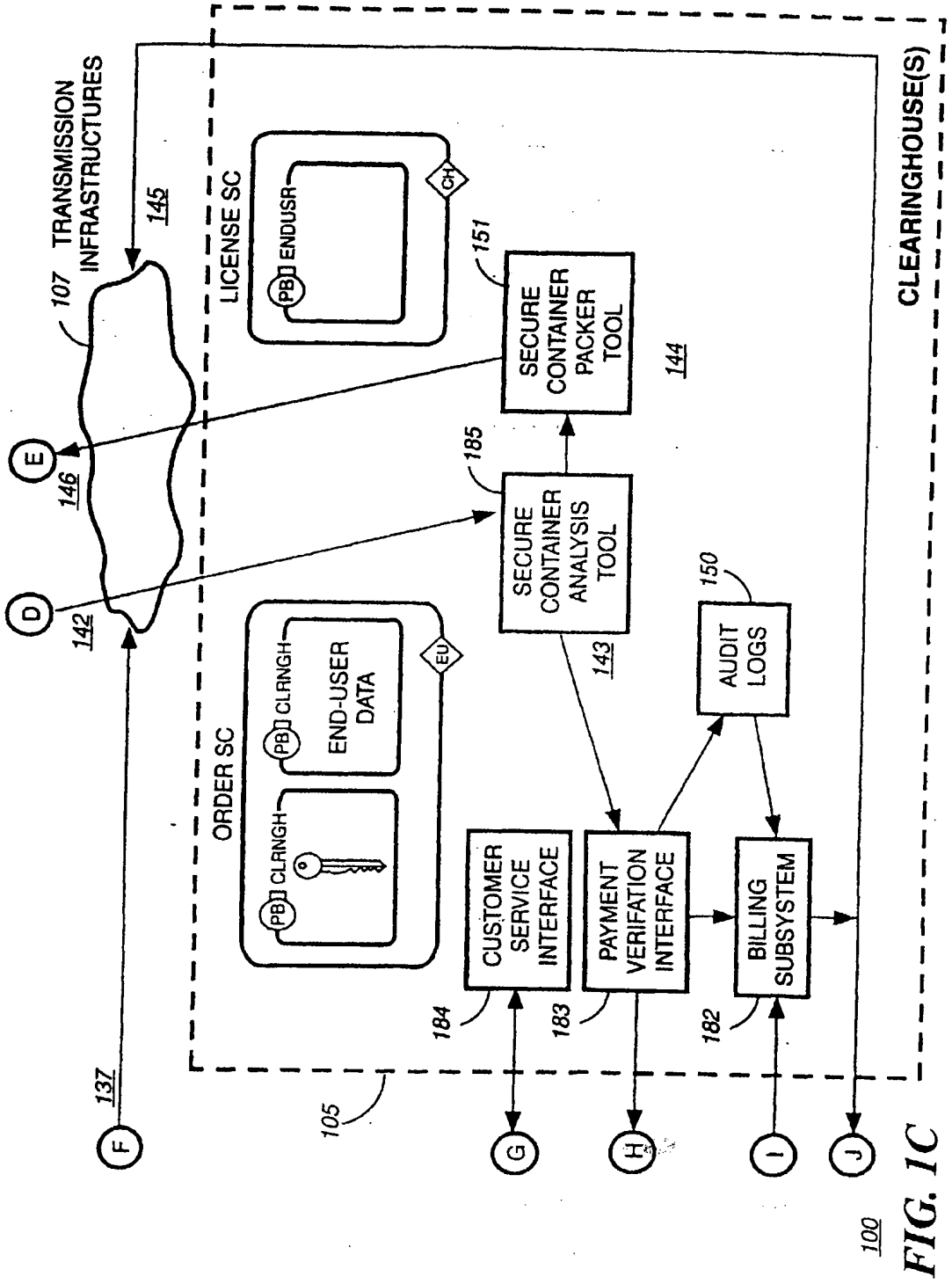

TRANSMISSION INFRASTRUCTURES
107
145
LICENSE SC
ENDUSR
CH
151
SECURE CONTAINER PACKER TOOL
144
CLEARINGHOUSE(S)
E
146
D
142
185
SECURE CONTAINER ANALYSIS TOOL
143
150
AUDIT LOGS
ORDER SC
CLRNGH
END-USER DATA
EU
CLRNGH
CUSTOMER SERVICE INTERFACE
PAYMENT VERIFATION INTERFACE
BILLING SUBSYSTEM
184
183
182
137
105
F
G
H
I
J
100

FIG. 1C

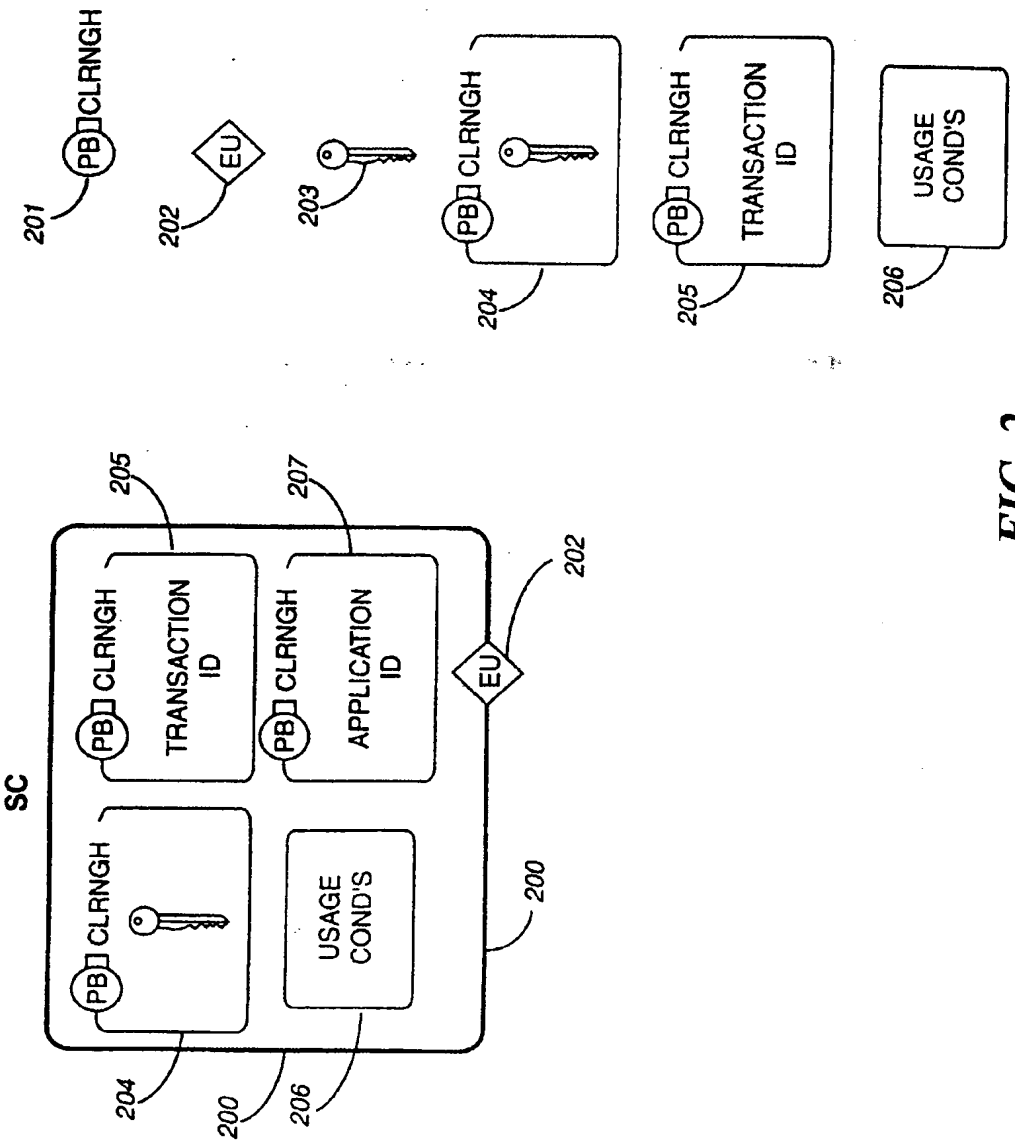

SC
PB CLRNGH
TRANSACTION ID
PB CLRNGH
APPLICATION ID
EU
PB CLRNGH
USAGE COND'S
200
202
204
205
206
207
201
203
PB CLRNGH
EU
PB CLRNGH
PB CLRNGH
TRANSACTION ID
USAGE COND'S

FIG. 2

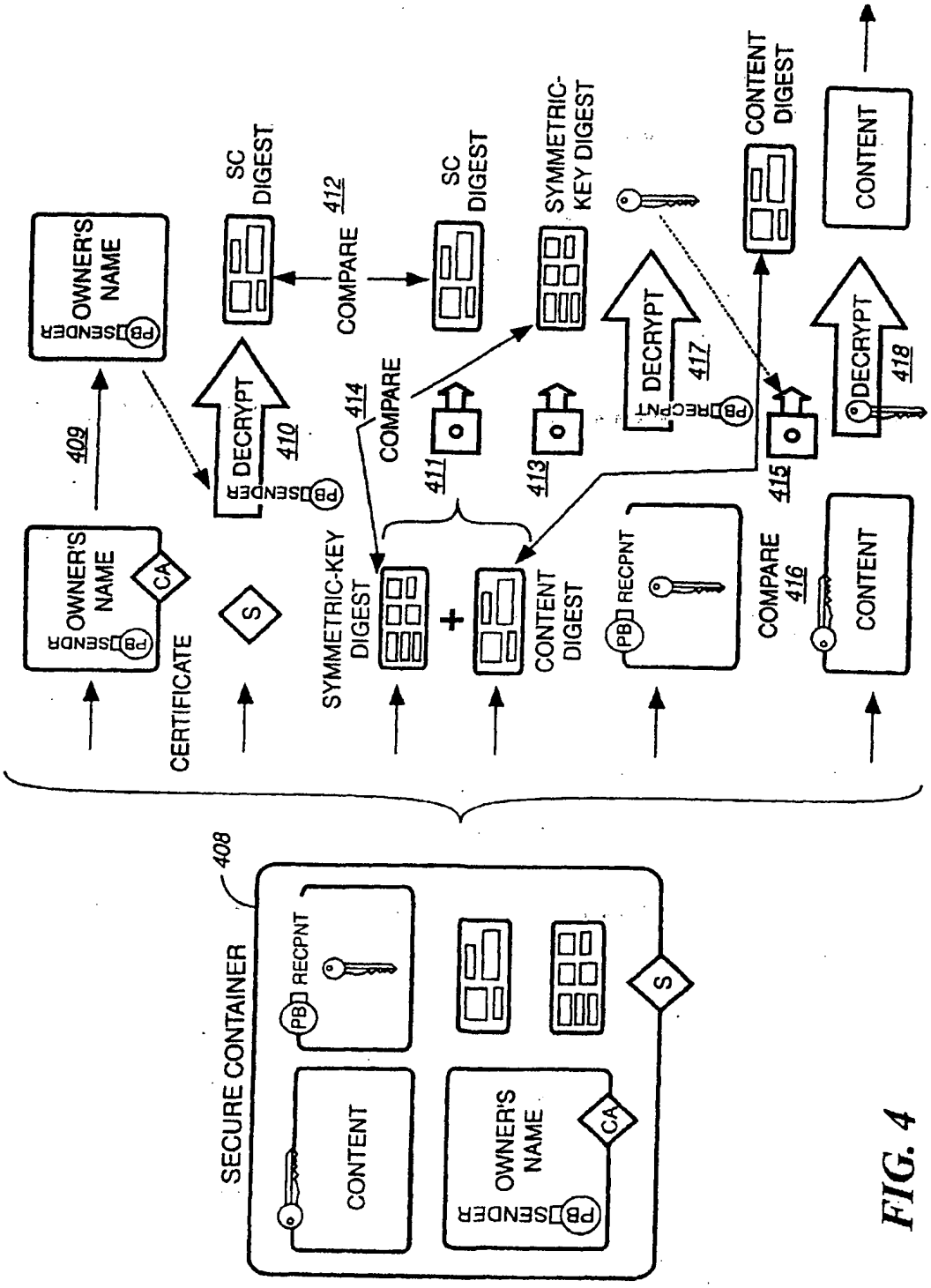

SECURE CONTAINER
408
CONTENT
PB RECPNT
OWNER'S NAME
PB SENDER
CA
S
CERTIFICATE
OWNER'S NAME
PB SENDER
CA
409
DECRYPT
PB SENDER
410
SC DIGEST
COMPARE
412
SC DIGEST
414
COMPARE
411
413
SYMMETRIC-KEY DIGEST
SYMMETRIC-KEY DIGEST
CONTENT DIGEST
PB RECPNT
DECRYPT
PB RECPNT
417
CONTENT DIGEST
415
COMPARE
416
CONTENT
DECRYPT
418
CONTENT

FIG. 4

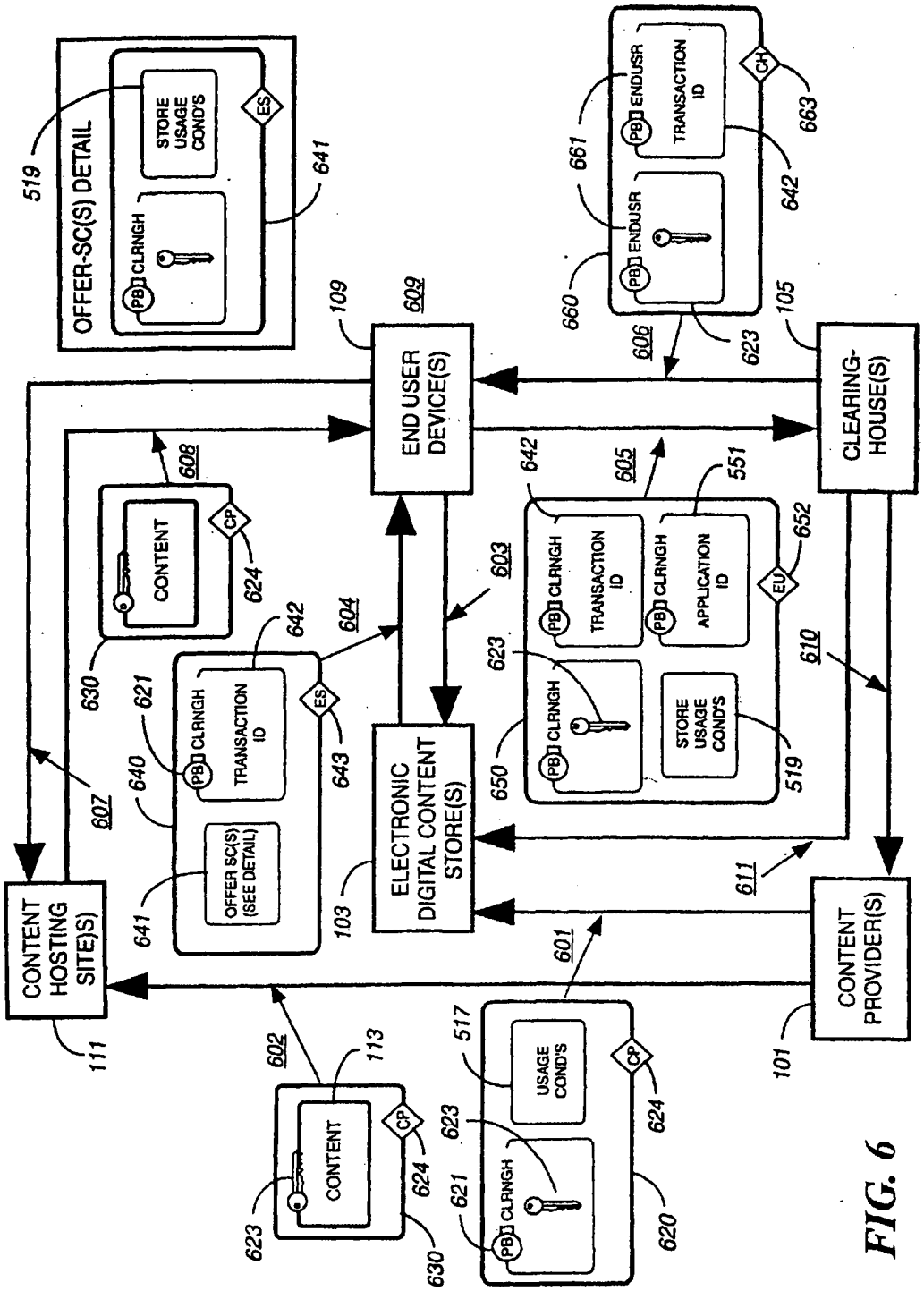

OFFER-SC(S) DETAIL
519
PB CLRNGH
STORE USAGE COND'S
ES
641
109
609
END USER DEVICE(S)
660
661
PB ENDUSR
PB ENDUSR
TRANSACTION ID
CH
663
642
606
623
105
CLEARING-HOUSE(S)
608
CONTENT
CP
624
630
642
605
551
652
603
604
PB CLRNGH
TRANSACTION ID
PB CLRNGH
APPLICATION ID
EU
623
621
640
PB CLRNGH
TRANSACTION ID
ES
643
650
PB CLRNGH
STORE USAGE COND'S
519
610
607
OFFER SC(S) (SEE DETAIL)
641
103
ELECTRONIC DIGITAL CONTENT STORE(S)
611
CONTENT HOSTING SITE(S)
601
CONTENT PROVIDER(S)
111
602
113
517
USAGE COND'S
CP
624
623
CONTENT
CP
624
621
PB CLRNGH
630
620
101

FIG. 6

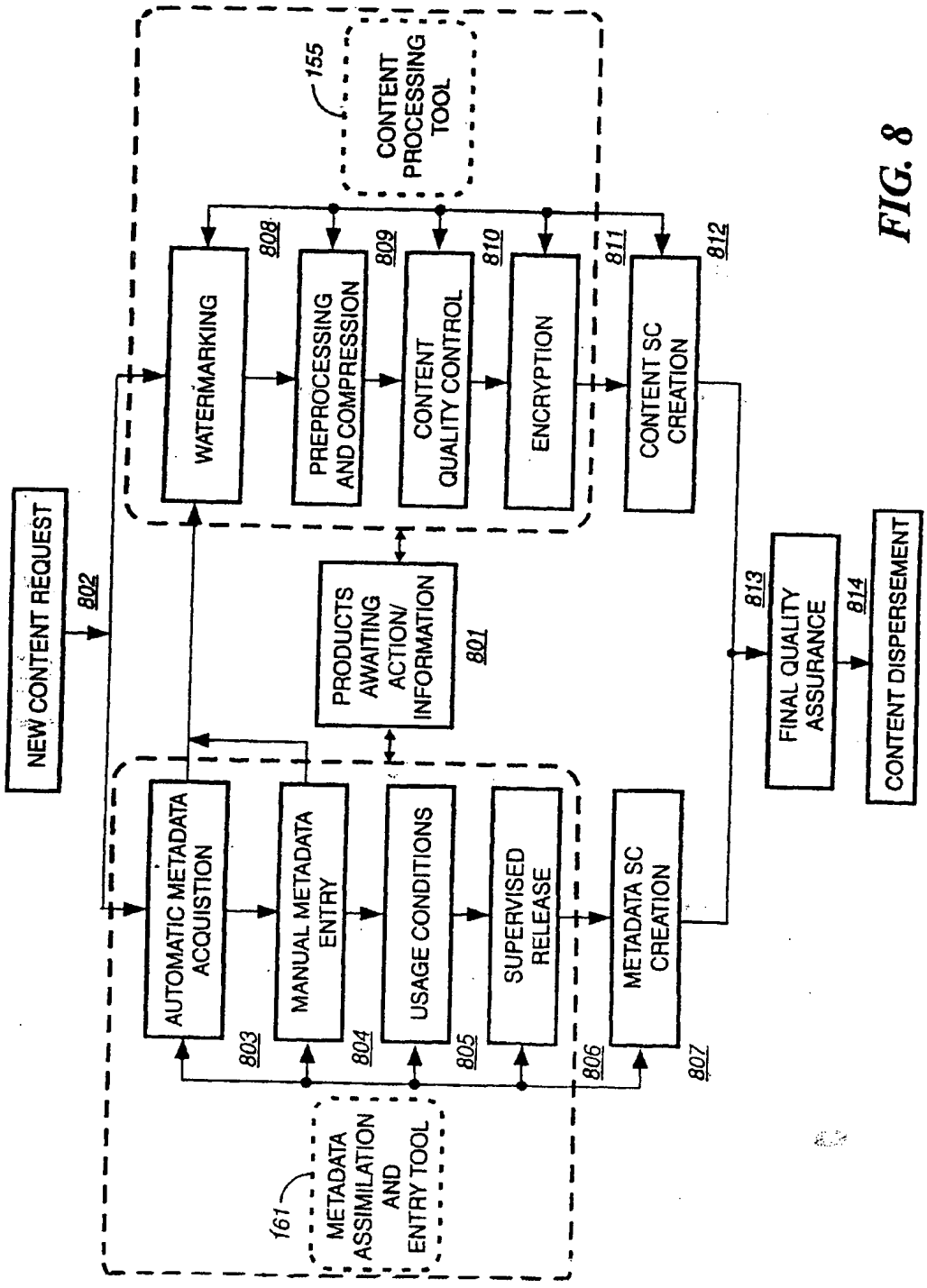

NEW CONTENT REQUEST
802
WATERMARKING
808
PREPROCESSING AND COMPRESSION
809
CONTENT QUALITY CONTROL
810
ENCRYPTION
811
CONTENT SC CREATION
812
CONTENT PROCESSING TOOL
155
PRODUCTS AWAITING ACTION/ INFORMATION
801
AUTOMATIC METADATA ACQUISTION
803
MANUAL METADATA ENTRY
804
USAGE CONDITIONS
805
SUPERVISED RELEASE
806
METADATA SC CREATION
807
METADATA ASSIMILATION AND ENTRY TOOL
161
FINAL QUALITY ASSURANCE
813
CONTENT DISPERSEMENT
814

FIG. 8

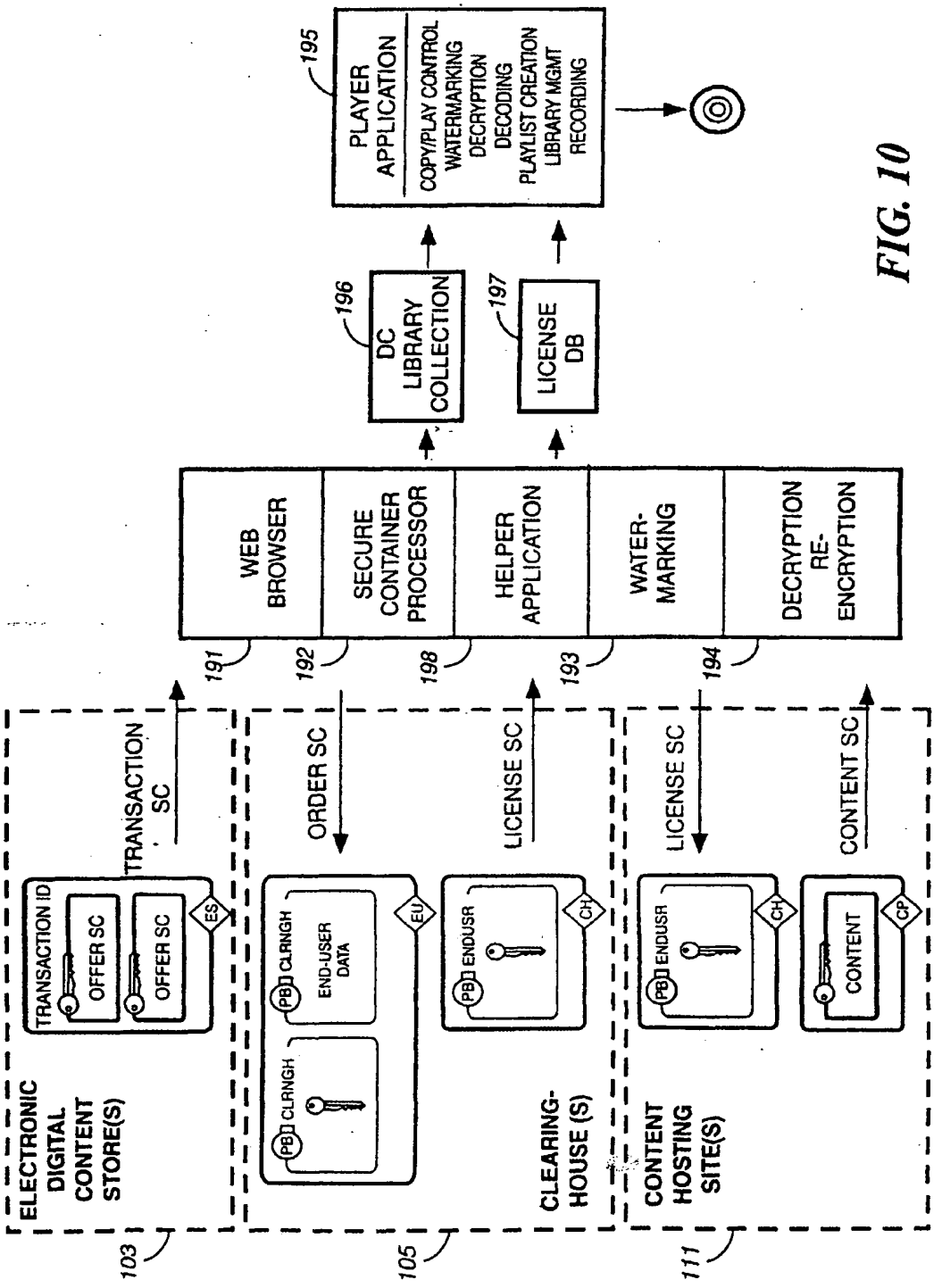

195
PLAYER APPLICATION
COPY/PLAY CONTROL
WATERMARKING
DECRYPTION
DECODING
PLAYLIST CREATION
LIBRARY MGMT
RECORDING
196
DC LIBRARY COLLECTION
197
LICENSE DB
WEB BROWSER
SECURE CONTAINER PROCESSOR
HELPER APPLICATION
WATER-MARKING
DECRYPTION RE-ENCRYPTION
191
192
198
193
194
TRANSACTION SC
ORDER SC
LICENSE SC
LICENSE SC
CONTENT SC
ELECTRONIC DIGITAL CONTENT STORE(S)
CLEARING-HOUSE (S)
CONTENT HOSTING SITE(S)
TRANSACTION ID
OFFER SC
OFFER SC
ES
PB
CLRNGH
END-USER DATA
EU
PB
CLRNGH
PB
ENDUSR
CH
PB
ENDUSR
CH
CONTENT
CP
103
105
111

FIG. 10

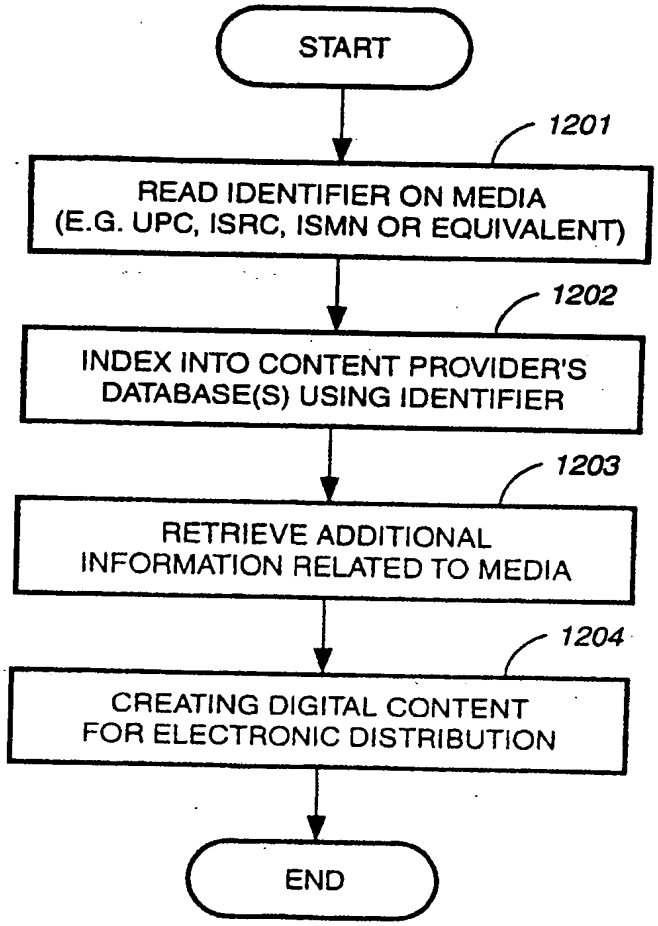

START
1201
READ IDENTIFIER ON MEDIA
(E.G. UPC, ISRC, ISMN OR EQUIVALENT)
1202
INDEX INTO CONTENT PROVIDER'S
DATABASE(S) USING IDENTIFIER
1203
RETRIEVE ADDITIONAL
INFORMATION RELATED TO MEDIA
1204
CREATING DIGITAL CONTENT
FOR ELECTRONIC DISTRIBUTION
END

FIG. 12

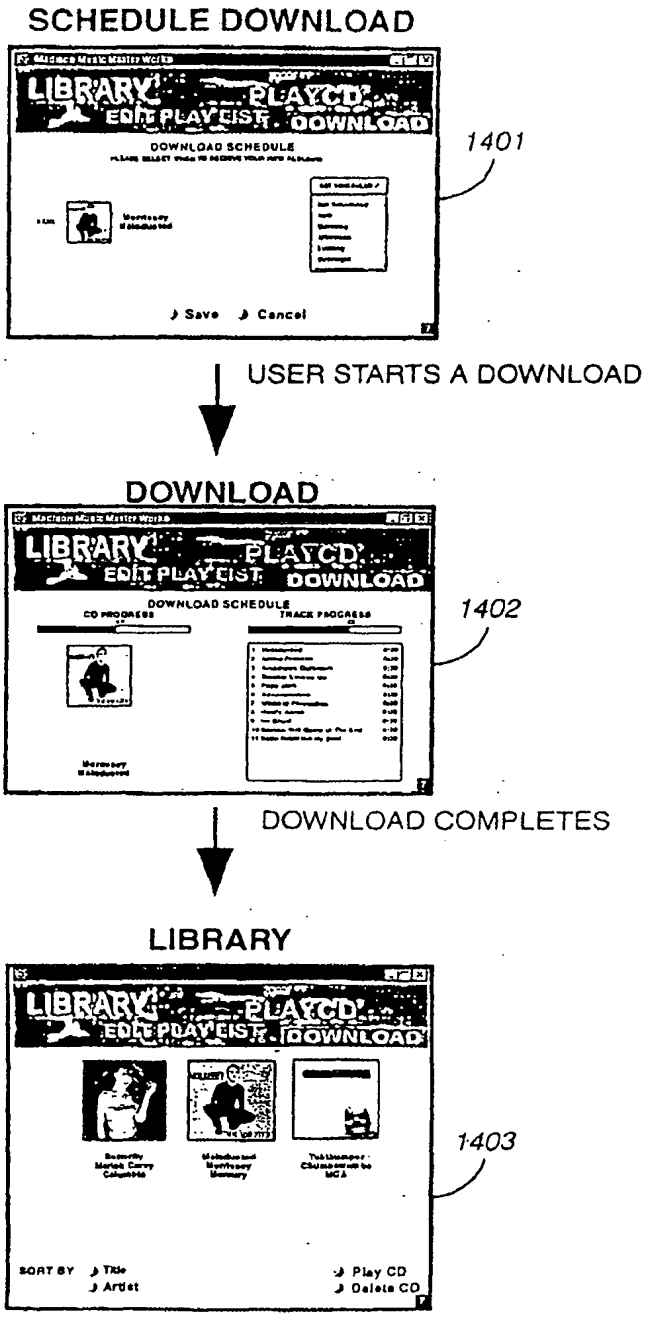

SCHEDULE DOWNLOAD
LIBRARY
PLAYCD
EDIT PLAYLIST
DOWNLOAD
DOWNLOAD SCHEDULE
Save
Cancel
1401
USER STARTS A DOWNLOAD
DOWNLOAD
LIBRARY
PLAYCD
EDIT PLAYLIST
DOWNLOAD
DOWNLOAD SCHEDULE
CD PROGRESS
TRACK PROGRESS
1402
DOWNLOAD COMPLETES
LIBRARY
LIBRARY
PLAYCD
EDIT PLAYLIST
DOWNLOAD
SORT BY
Title
Artist
Play CD
Delete CD
1403

FIG. 14

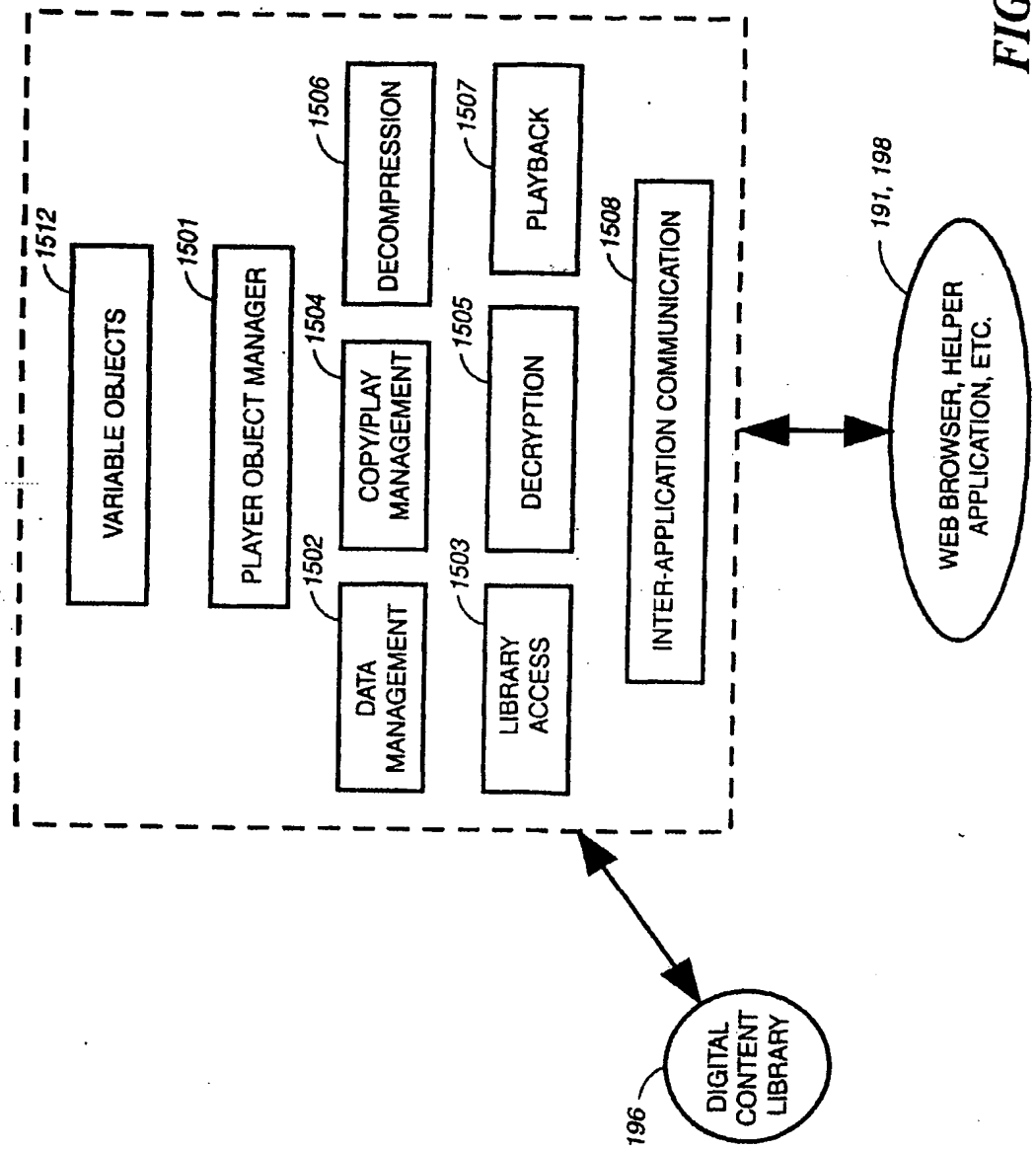

1512
VARIABLE OBJECTS
1501
PLAYER OBJECT MANAGER
1502
DATA MANAGEMENT
1504
COPY/PLAY MANAGEMENT
1503
LIBRARY ACCESS
1506
DECOMPRESSION
1505
DECRYPTION
1507
PLAYBACK
1508
INTER-APPLICATION COMMUNICATION
191, 198
WEB BROWSER, HELPER APPLICATION, ETC.
196
DIGITAL CONTENT LIBRARY

FIG. 15B

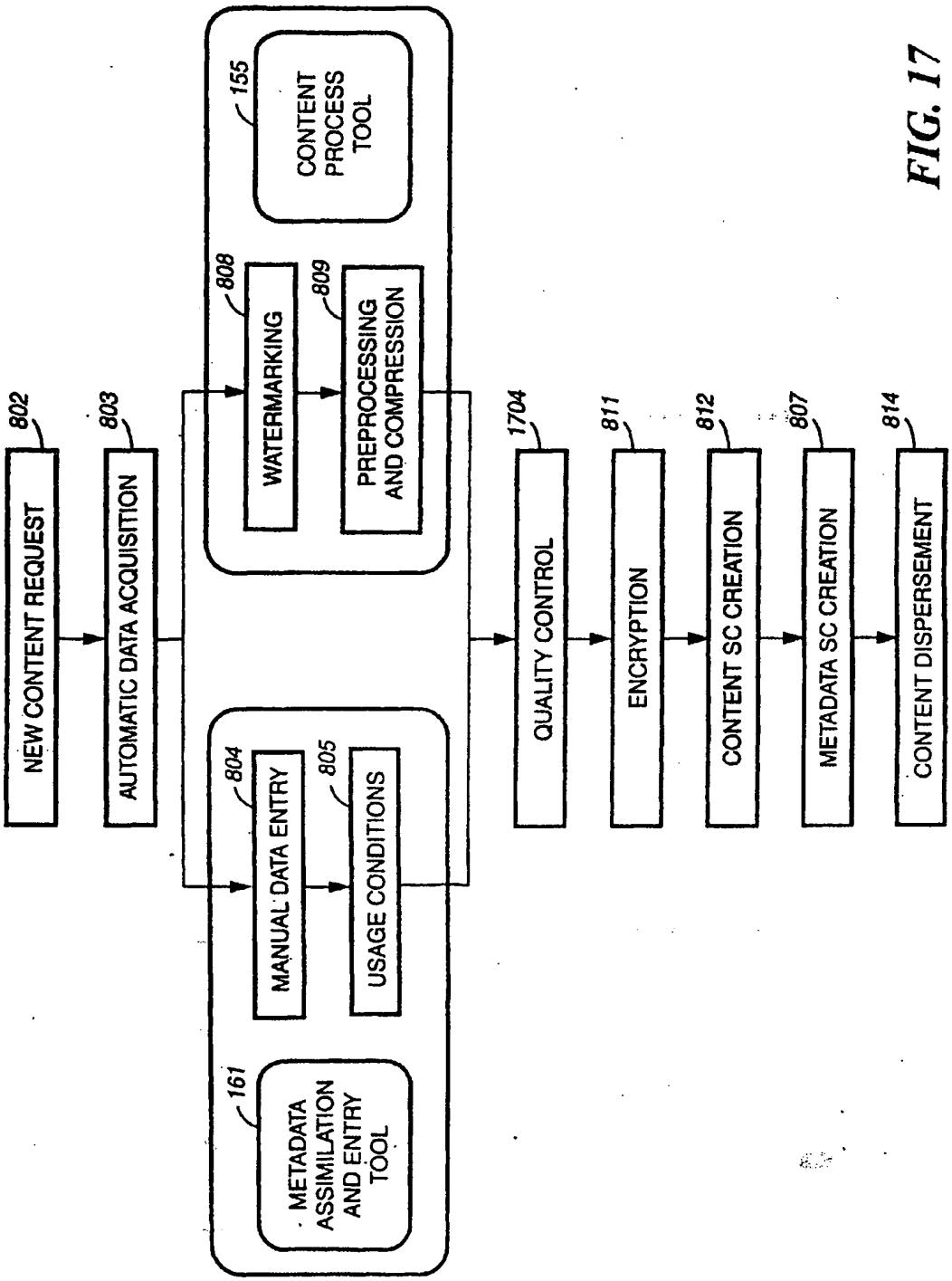

802
NEW CONTENT REQUEST
803
AUTOMATIC DATA ACQUISITION
155
CONTENT PROCESS TOOL
808
WATERMARKING
809
PREPROCESSING AND COMPRESSION
804
MANUAL DATA ENTRY
805
USAGE CONDITIONS
161
METADATA ASSIMILATION AND ENTRY TOOL
1704
QUALITY CONTROL
811
ENCRYPTION
812
CONTENT SC CREATION
807
METADATA SC CREATION
814
CONTENT DISPERSEMENT

FIG. 17

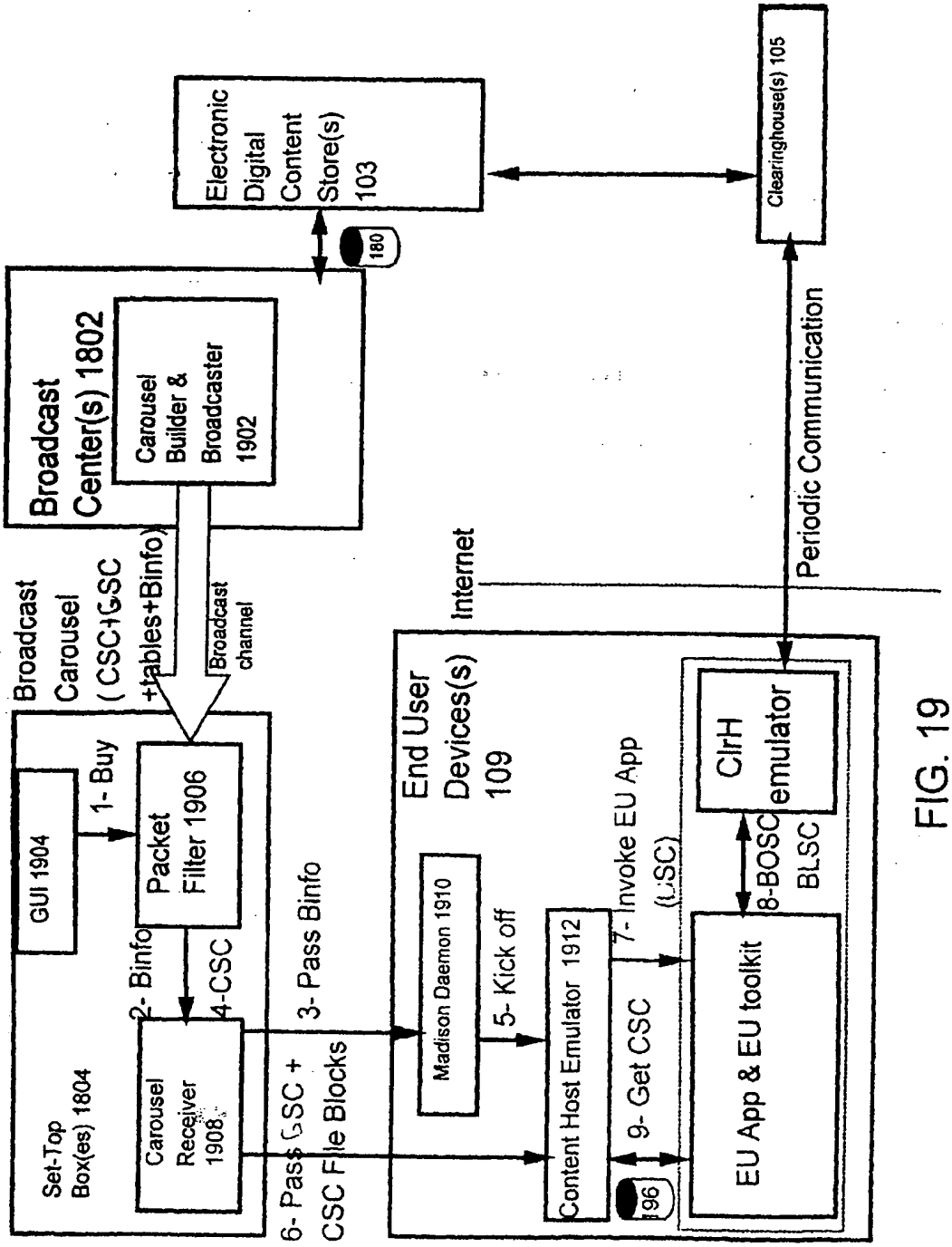

Electronic Digital Content Store(s) 103
180
Clearinghouse(s) 105
Broadcast Center(s) 1802
Carousel Builder & Broadcaster 1902
Broadcast Carousel (CSC+GSC +tables+Binfo)
Broadcast channel
Internet
Periodic Communication
Set-Top Box(es) 1804
GUI 1904
1- Buy
Packet Filter 1906
2- Binfo
4-CSC
Carousel Receiver 1908
3- Pass Binfo
6- Pass GSC + CSC File Blocks
End User Devices(s) 109
Madison Daemon 1910
5- Kick off
Content Host Emulator 1912
7- Invoke EU App (LSC)
9- Get CSC
196
EU App & EU toolkit
8-BOSC
BLSC
ClrH emulator

FIG. 19

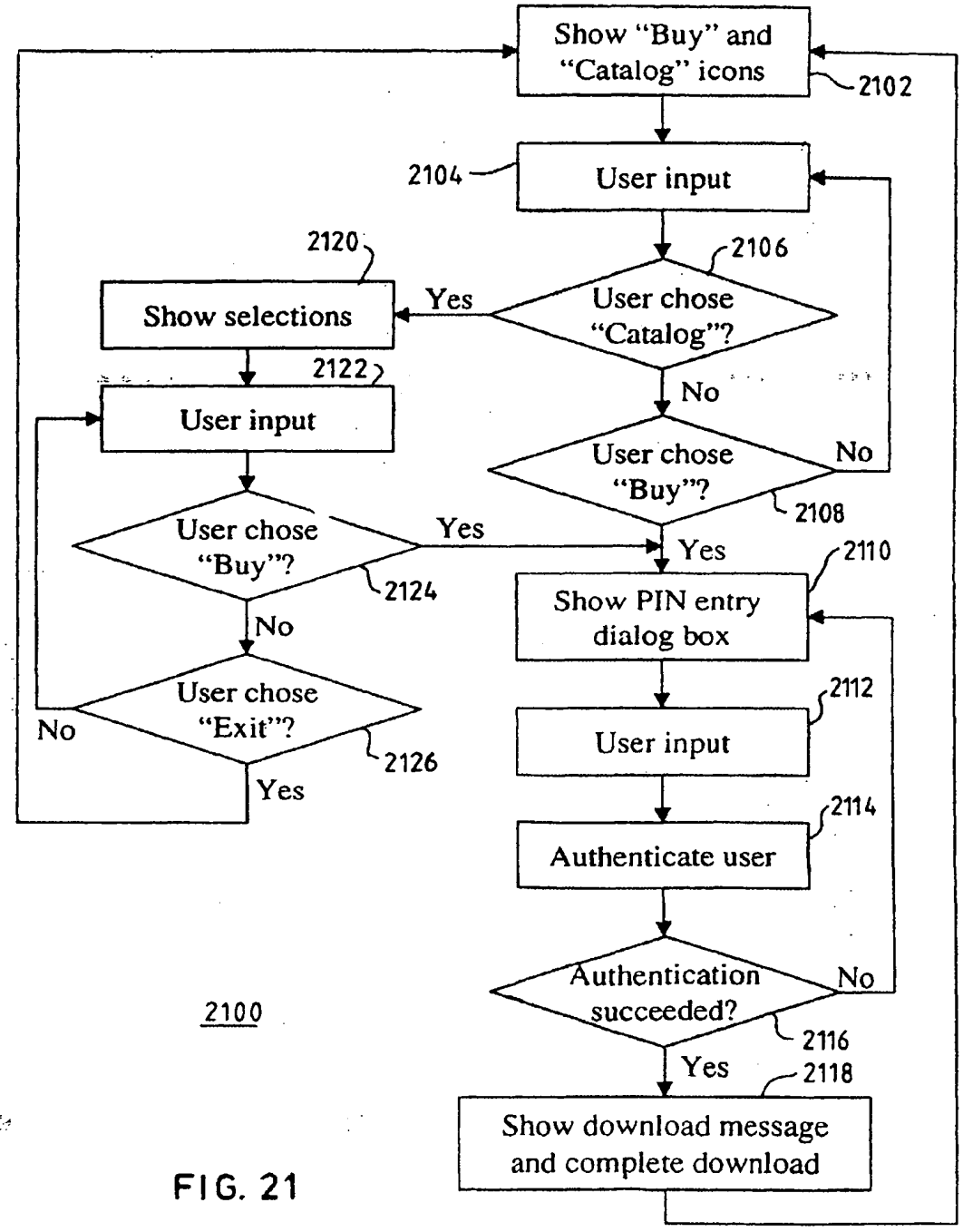

Show "Buy" and "Catalog" icons
2102
2104
User input
2106
User chose "Catalog"?
Yes
2120
Show selections
No
2122
User input
User chose "Buy"?
No
2108
Yes
User chose "Buy"?
Yes
2124
No
2110
Show PIN entry dialog box
User chose "Exit"?
No
2126
Yes
2112
User input
2114
Authenticate user
Authentication succeeded?
No
2116
Yes
2118
Show download message and complete download
2100

FIG. 21

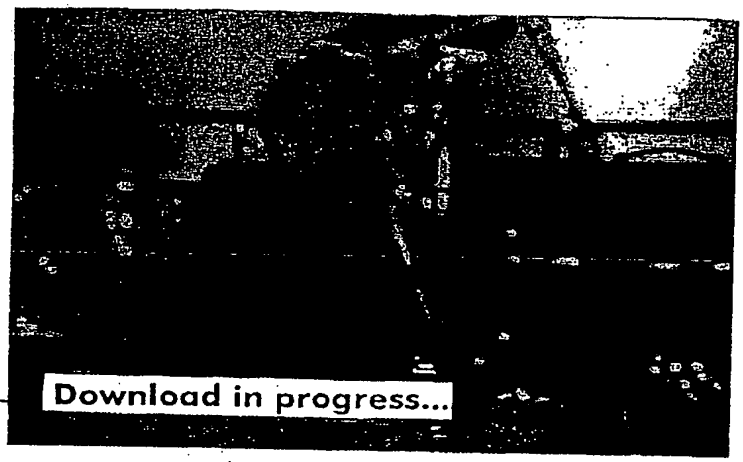

2404
Download in progress...

FIG. 26

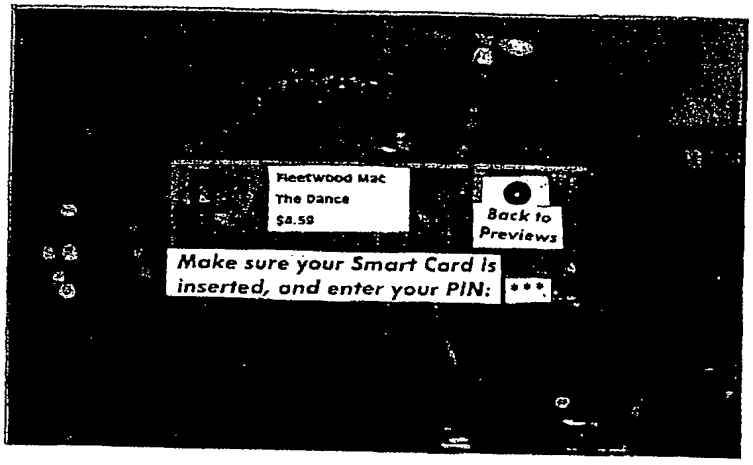

Fleetwood Mac
The Dance
$8.59
Back to Previews
Make sure your Smart Card is inserted, and enter your PIN:
***

FIG. 24

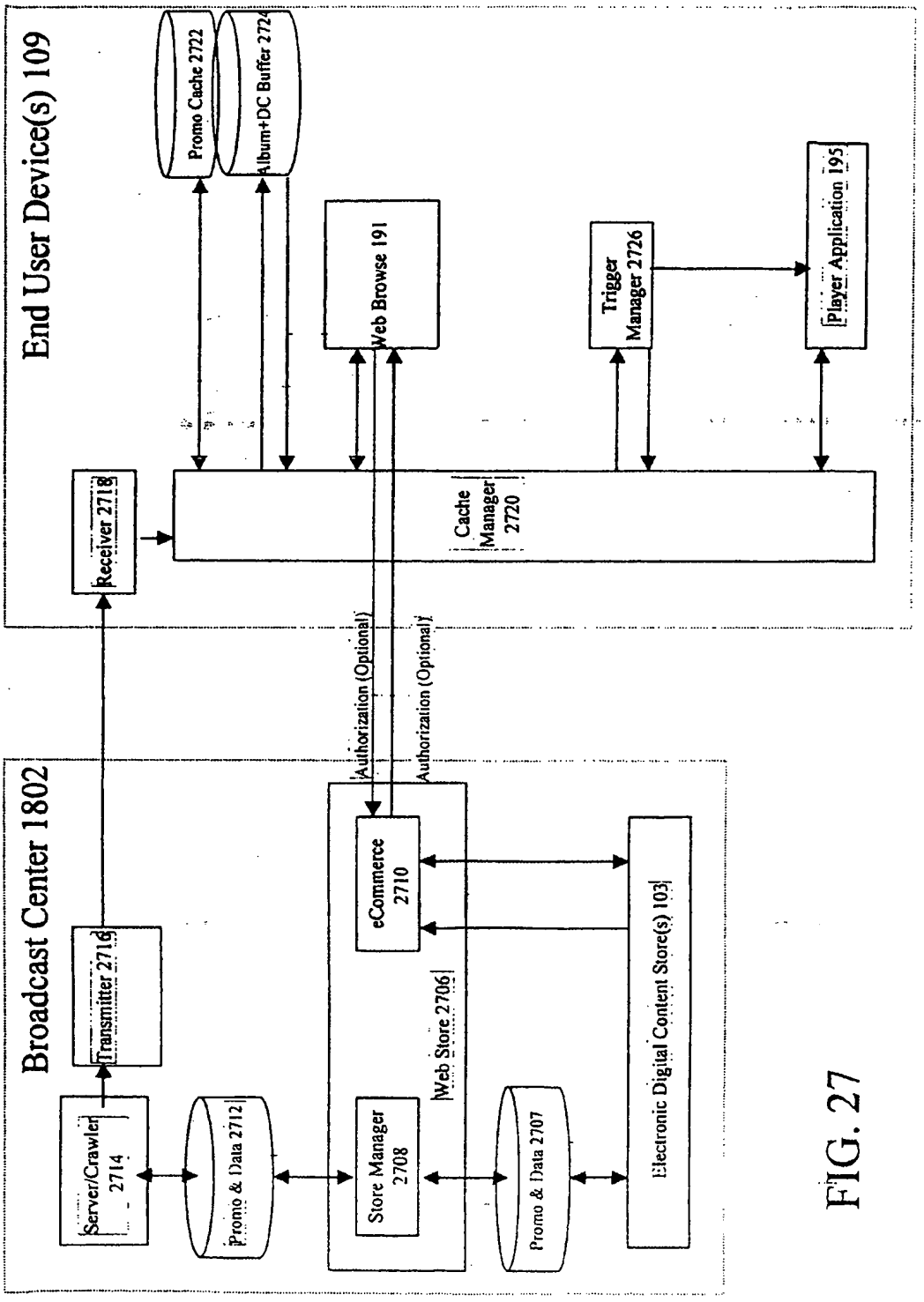

End User Device(s) 109
Promo Cache 2722
Album+DC Buffer 2724
Web Browse 191
Trigger Manager 2726
Player Application 195
Receiver 2718
Cache Manager 2720
Authorization (Optional)
Authorization (Optional)
Broadcast Center 1802
Transmitter 2716
eCommerce 2710
Server/Crawler 2714
Promo & Data 2712
Store Manager 2708
Web Store 2706
Promo & Data 2707
Electronic Digital Content Store(s) 103

FIG. 27

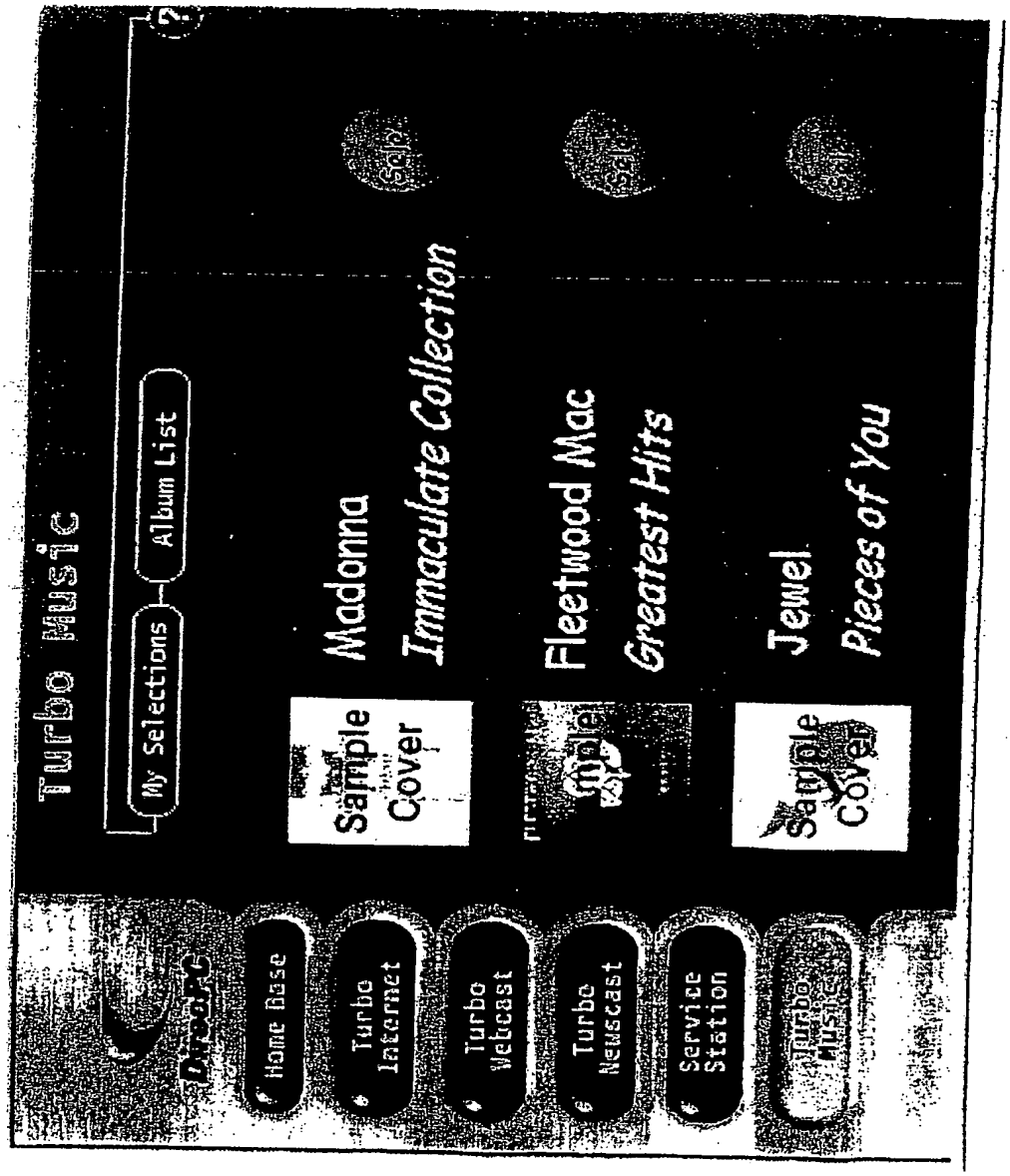
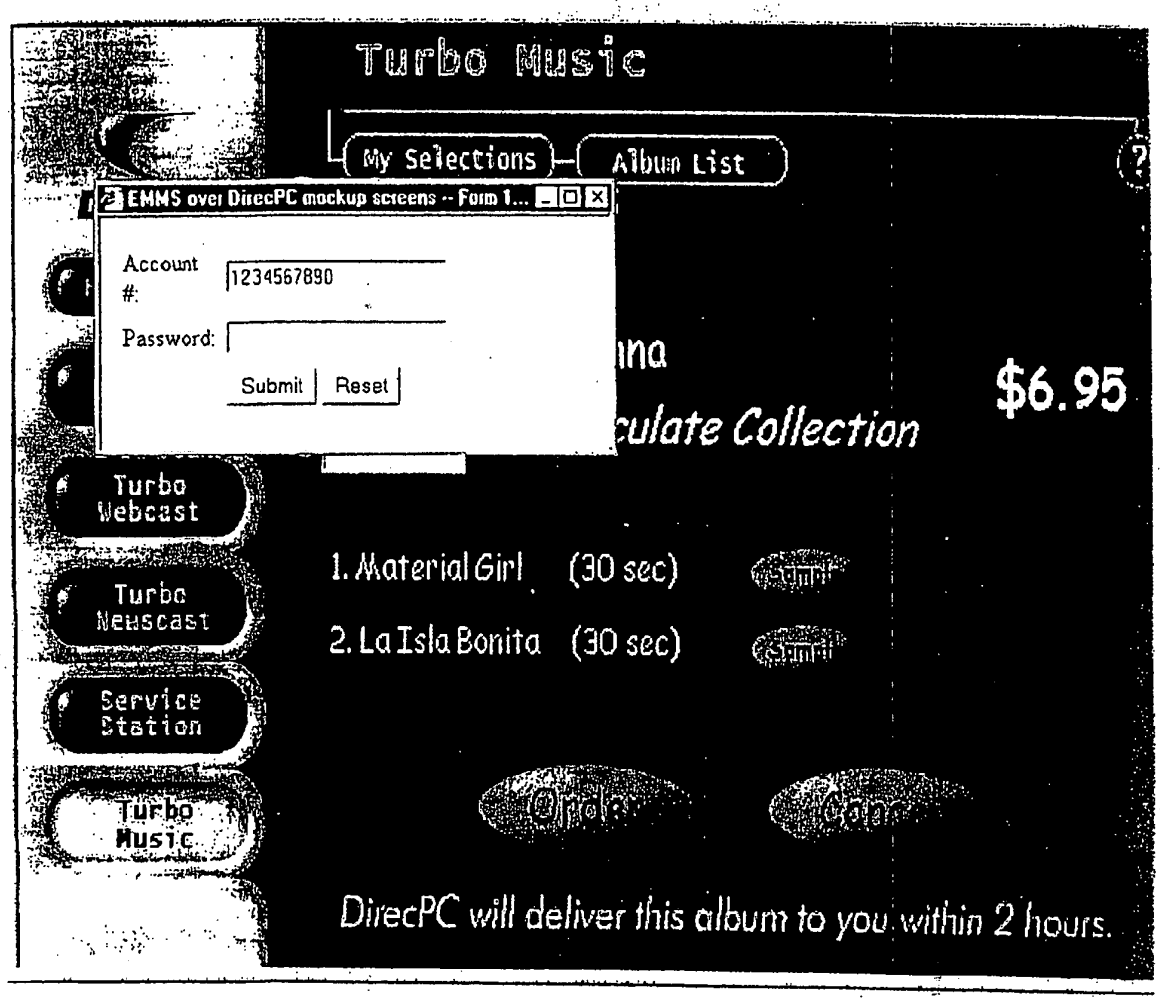

Turbo Music
My Selections
Album List
Home Base
Turbo Internet
Turbo Webcast
Turbo Newscast
Service Station
Turbo Music
Sample Cover
Madonna
Immaculate Collection
Fleetwood Mac
Greatest Hits
Jewel
Pieces of You

FIG. 29


Turbo Music
My Selections
Album List
EMMS over DirecPC mockup screens -- Form 1...
Account #:
1234567890
Password:
Submit
Reset
$6.95
culate Collection
Turbo Webcast
Turbo Newscast
Service Station
Turbo Music
1. Material Girl (30 sec)
2. La Isla Bonita (30 sec)
DirecPC will deliver this album to you within 2 hours.

115

FIG. 31

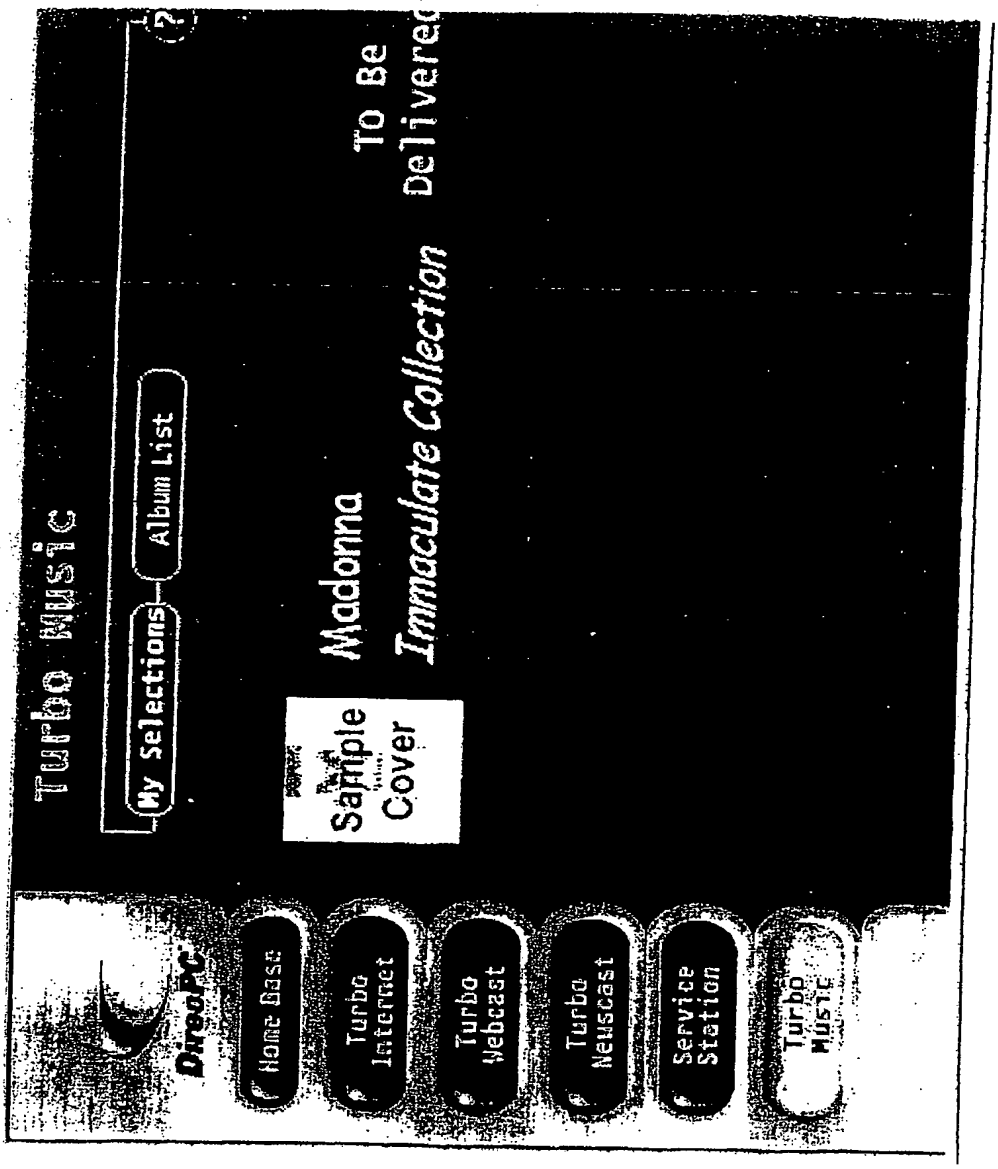

Turbo Music
My Selections
Album List
Sample Cover
Madonna
Immaculate Collection
To Be Delivered
Home Base
Turbo Internet
Turbo Webcast
Turbo Newscast
Service Station
Turbo Music

FIG. 33

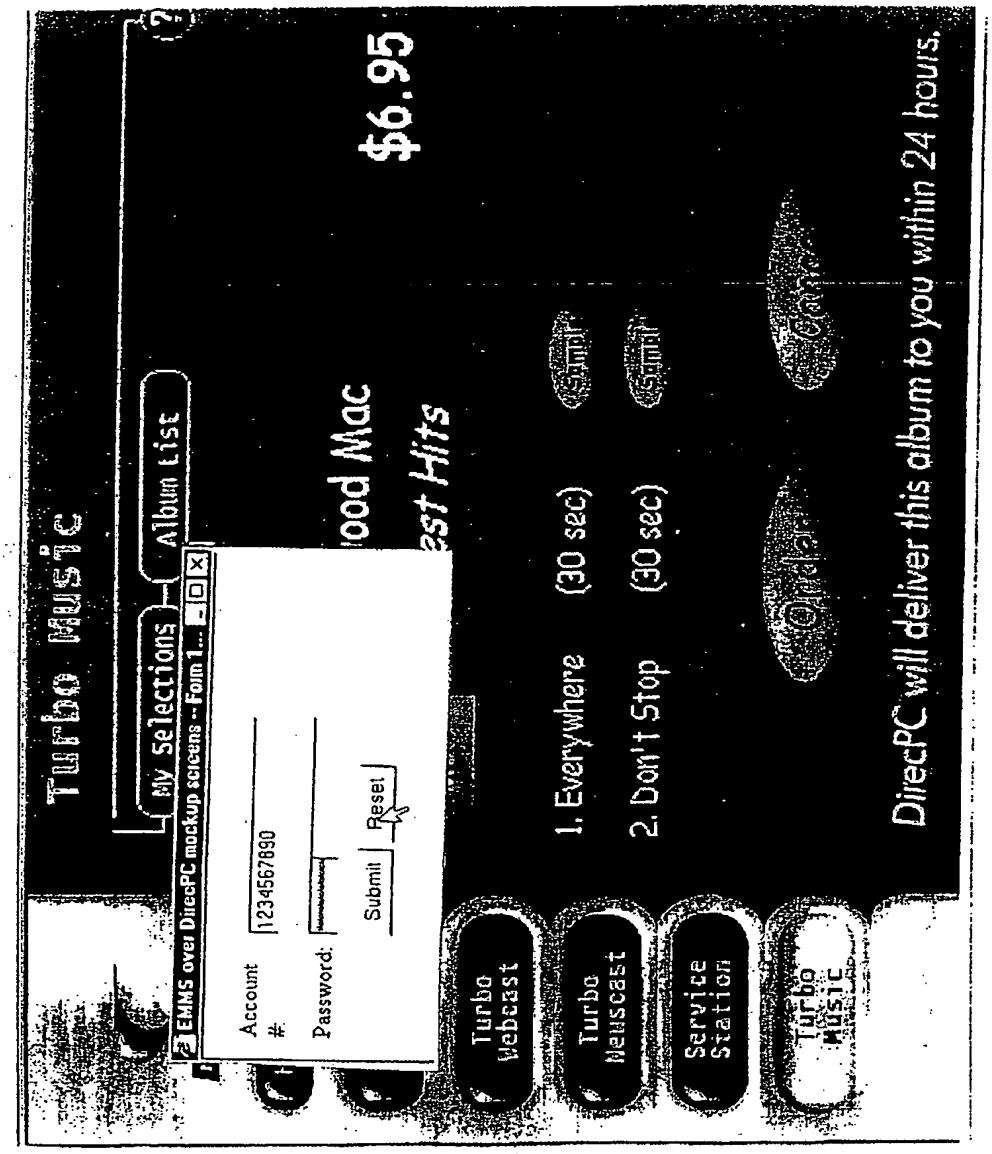

Turbo Music
My Selections
Album List
EMMS over DirecPC mockup screens -- Form 1...
Account #
1234567890
Password:
Submit
Reset
ood Mac
est Hits
$6.95
1. Everywhere (30 sec)
2. Don't Stop (30 sec)
Sample
Sample
Order
Cancel
DirecPC will deliver this album to you within 24 hours.
Turbo Webcast
Turbo Newscast
Service Station
Turbo Music

FIG. 35

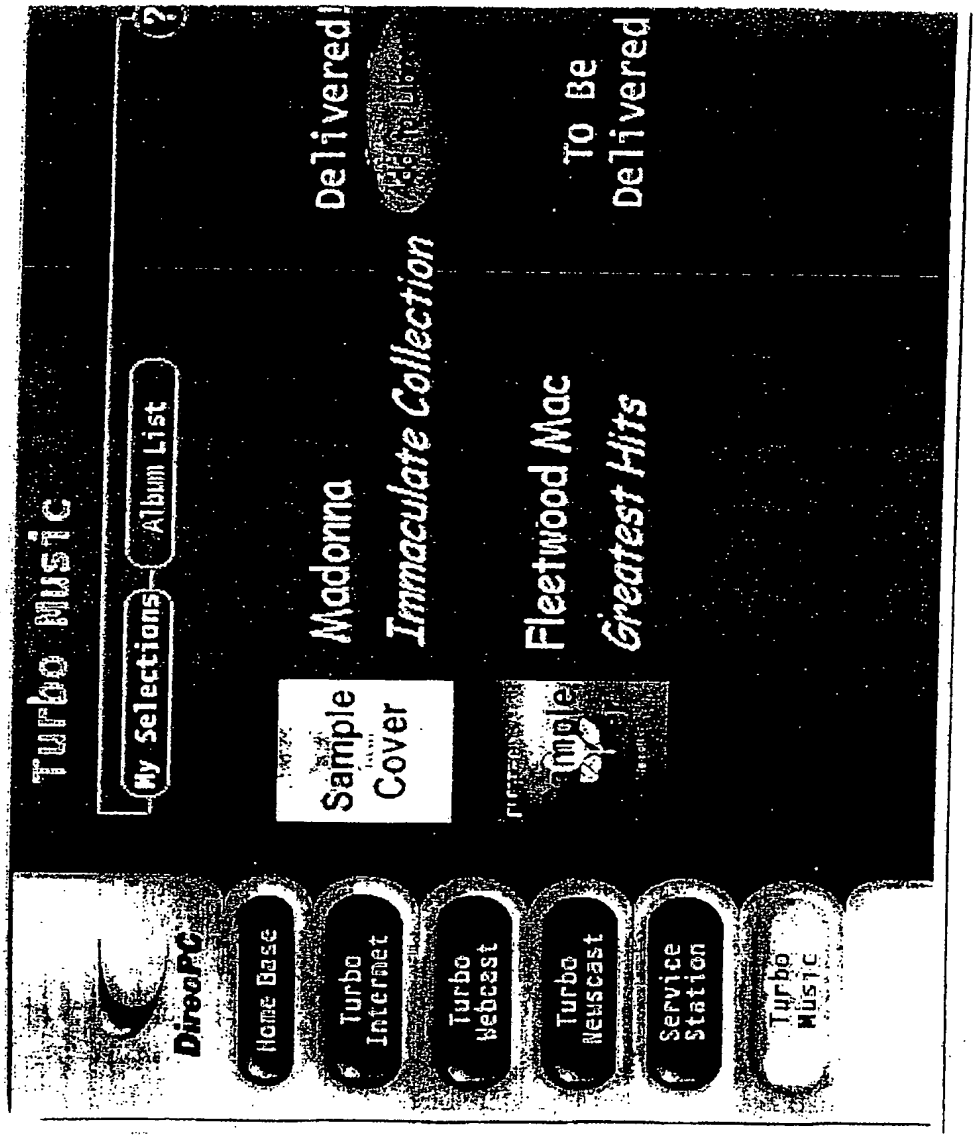

Turbo Music
My Selections
Album List
DirecPC
Home Base
Turbo Internet
Turbo Webcast
Turbo Newscast
Service Station
Turbo Music
Sample Cover
Madonna
Immaculate Collection
Delivered
Fleetwood Mac
Greatest Hits
To Be Delivered

FIG. 37